

VISIT...

LANZAROTE
Caliente.COM

USING RADIO FREQUENCY IDENTIFICATION (RFID) TECHNOLOGY
IN HUMANS IN THE UNITED STATES FOR
TOTAL CONTROL

by

David B. Smith

A Graduate Research Report Submitted for INSS 690
in Partial Fulfillment of the Requirements of the Degree of
Master of Science in Management Information Systems

Bowie State University
Maryland in Europe
July 2006

TABLE OF CONTENTS

	Page
ABSTRACT	iii
LIST OF FIGURES	iv
CHAPTER	
I INTRODUCTION	
Statement of Problem	1
Need for the Study	1
Definition of the Terms	1
II REVIEW OF THE LITERATURE	
Sources Used for Review of Literature	4
Questions Used for Review of Literature	4
Review of Sources of Literature	4
Summary of the Literature	19
Research Hypothesis	19
III METHODOLOGY	
Design	20
Procedures	20
Assumptions & Limitations	20
V ANALYSIS AND DISCUSSION	
RFID Basics	
Definition	21
History	21
Types of Tags/Chips	22
RFID System	25
RFID Usage	26
Potential Usage	28
Standards	29
Technological Issues	
Performance	30
Security	35
Ramifications	
Medical	38
Business	39
Political	40
Legal	42
Religious	43
VI CONCLUSIONS AND RECOMMENDATIONS	44
REFERENCES	45
AUTHOR'S NOTE	53

ABSTRACT

Radio Frequency Identification (RFID) technology is not new, yet few people outside of manufacturing and privacy rights groups know much about it. RFID, a subset of the auto-identification technologies available, is increasingly being used by the U.S. government in electronic identification cards, passports and vehicle identification. These new and possibly nefarious uses of RFID raise serious security and privacy issues, and are brought to us by the same government as the Patriot Act and warrantless phone surveillance. Is the U.S. government headed in the direction of past police states such as Nazi Germany and Cuba? In this paper, this question as well as other security and privacy concerns will be analyzed and discussed.

LIST OF FIGURES

	Page
Figure 1 – RFID Microchip Implant	24
Figure 2 – RFID Tags in Various Shapes and Sizes	25
Figure 3 – RFID Temperature Sensing Tag	27
Figure 4 - RFID Tags Used in Libraries	28
Figure 5 – RFID Near Field Communication	34
Figure 6 – RFID Far Field Communication	35
Figure 7 – RFID CYPACK Chip (Commercial – In Use Today)	37
Figure 8 – RFID Blocking Wallet	37
Figure 9 – RFID Blocking Passport Case	37

CHAPTER ONE INTRODUCTION

Statement of the Problem

Radio Frequency Identification (hereafter referred to as RFID) is an automatic identification technology being used in manufacturing and supply chain management to control inventory information and control processes. Major initiatives by large corporations (such as Wal-Mart and Proctor & Gamble) and the U.S. government (to include the Department of Defense) have raised both public consciousness and fears of RFID technology and its current and potential uses.

Large corporations view RFID as an easy way to improve their internal operations and provide additional services for their customers. Potential benefits of RFID for large corporations include faster processing of their inventory with fewer errors, identification of counterfeit products and internal theft, and a faster checkout and overall better experience by consumers.

The U.S. government views RFID as a means to streamline the inventory acquisition and control process, to provide secure identity checks, improve the control on clandestine immigration and reduce potential misidentification. They also view RFID as a potential tool in the fight against terrorism, and this is where the largest point of contention is amongst the myriad politicians, courts, privacy advocates, corporations, pundits and individual citizens.

Need for the Study

In light of the potential privacy and security misuse by the government, I propose the need to study these issues in-depth to gain insight as to where the U.S. government is headed with this technology.

Definition of the Terms

ACLU: American Civil Liberties Union, a civil liberties organization in the United States.

Active RFID Tag: An RFID tag that has its own internal power source.

AMA: American Medical Association.

CASPIAN: Consumers Against Supermarket Privacy Invasion and Numbering, a privacy advocate organization currently headed by Katherine Albrecht.

CMOS: Complementary Metal Oxide Semiconductor, a small, battery-backed memory bank in a computer that holds configuration settings.

Collision: 2 IDs transmitted at the same time.

EEPROM: Electrically Erasable Programmable Read Only Memory, a rewritable memory chip that holds its content without power. EEPROMs have a lifespan of between 10K and 100K write cycles, which is considerably greater than the E-PROMs that preceded them.

EFF: Electronic Frontier Foundation, a privacy rights organization.

EPC: Electronic Product Code; a code electronically recorded on an RFID tag. It is intended to be an improvement on the UPC barcode system. The EPC is a 64- or 96-bit code, which based on current numbering schemes (Global Trade Item Number, VIN etc.), is divided into numbers that differentiate the product and manufacturer of a given item. The difference between EPC and previous numbering systems lies in the usage of an extra set of digits to uniquely identify one object. An EPC number contains: A Header, identifying the length, type, structure, version and generation of EPC; the Manager Number, which identifies the company or company entity; Object Class, similar to a Stock Keeping Unit or SKU; and a Serial Number, which is the specific instance of the Object Class being tagged. The Electronic Product Code promises to become the standard for global RFID usage. The EPC was the creation of the MIT Auto-ID Center, a consortium of over 120 global corporations and university labs. The EPC system is currently managed by EPCglobal, Inc., a subsidiary of GS1, creators of the UPC barcode.

FCC: Federal Communications Commission, an electronic communications agency of the United States..

Frequency: The number of cycles per second, usually measured in Hertz.

Gen 2: Current international standards for the use of RFID and EPC approved by the EPCGlobal joint venture operated by GS1.

GS1: The organization operating the joint venture EPCGlobal, with representatives from GS1, GS1-US, EAN, UCC, The Gillette Company, Proctor & Gamble, Wal-Mart, Hewlett-Packard, Johnson & Johnson, Checkpoint Systems, Auto-ID Labs and others.

HTML: Hyper-Text Mark-up Language.

IFF: Identification of Friend or Foe (an RFID-like system invented by the British in 1939 for use during World War II to identify airplanes as friend or foe).

ISM Bands: Industrial, Scientific and Medical frequency bandwidths commonly used – 128 KHz, 13.56 MHz, 915 MHz and 2.45 GHz.

ISO: International Standards Organization, the organization that sets standards in many businesses and technologies, including computing and communications.

Passive RFID Tag: An RFID tag that has no internal power supply.

PML: Physical Markup Language, an XML-based language that is used to define data on objects.

POS: Point-of-Sale; a cashier system used by the majority of businesses.

RFID: Radio Frequency Identification, an auto-identification technology.

ROI: Return on Investment; a financial term used to decide whether to fund a project or not.

SCM: Supply Chain Management; the planning, scheduling and control of the supply chain, which is the sequence of organizations and functions that mine, make or assemble materials and products from manufacturer to wholesaler to retailer to consumer. The driving force behind supply chain management (SCM) is to reduce inventory.

Semi-Passive RFID Tag: Similar to a Passive RFID tag with the addition of a small battery.

UHF: Ultra-High Frequency, with frequencies ranging from 300 MHz to 3 GHz.

XML: Extensible Mark-up Language, a more flexible version of HTML.

CHAPTER TWO

REVIEW OF THE LITERATURE

Sources Used for Review of the Literature

The sources of literature reviewed for this study include major news outlets, technology websites and journals, consolidated federal and civilian law databases, educational journals, websites and databases, and personal websites and blogs. To avoid slanting this research paper in any particular direction, multiple overlapping sources were used so that most viewpoints on the technology and ramifications would be included.

Questions Used for Review of Literature

RFID Basics

What is RFID technology – definition, history, types, RFID system, usage, potential uses, standards and regulations?

Technological Issues

What are the technological issues of using RFID technology in humans?

Ramifications

What are the ramifications of using RFID technology in humans for immigration and control (medical, business, political, legal and religious)?

Review of Sources of Literature

RFID Basics Sources

RFID – From Wikipedia, the free encyclopedia. This source was very useful for *RFID Basics* (definition, history, types, system, and usage); it was also useful for listing potential uses, current regulations and standardization, and RFID legislation. There were no *Technological Issues* addressed in this source. It was only slightly useful for *Ramifications*. This source is constantly being updated. <http://en.wikipedia.org/wiki/RFID>

Protecting your ID – RFID chip in humans get green light. The author of this article is Alorie Gilbert, a writer for CNET Networks. This article covers the FDA approval for the medical use of injecting humans with tracking devices, and is a good source for *Ramifications* (medical, business, legal and ethical).

<http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39124983,00.htm>

The long road to RFID interoperability. The author of this article is James R. Borck, and is the first of two articles written on the same day. This article covers the Generation 2 standard for RFID, and is a good source for *RFID Basics* (standards) and *Ramifications* (business).

http://www.infoworld.com/infoworld/article/06/04/13/77022_16FErfidsoftgen2_1.html

Next-gen RFID tools expand the market – New standards, software help RF-enable business of any size. The author of this article is James R. Borck, and is the second of two articles written on the same day. This article goes more in-depth into the Generation 2 standards, and is a good source for *RFID Basics* (standards) and *Ramifications* (business).

http://www6.infoworld.com/products/print_friendly.jsp?link=/article/06/04/13/77019_16FErfidsoft_1.html

Technological Issues Sources

The Magic of RFID. The author of this article is Roy Want, a principal engineer at Intel Research. This article is the technical background of RFID and is a good source for *Technological Issues*.

<http://delivery.acm.org.ezproxy.umuc.edu/10.1145/1040000/1035619/p40-want.pdf?key1=1035619&key2=4638308411&coll=GUIDE&dl=ACM&CFID=71690688&CFTOKEN=99404625>

AIM Global Sources

AIM Global is the industry association and worldwide authority on automatic identification and mobility technologies. AIM members are providers and users of technologies, systems, and services that capture, manage, and integrate accurate data into larger information systems. There are more than 900 members in 43 countries. These reviews are in chronological order according to date of publication.

Analysis: Counterfeit Tags. Question and answer session with RFID expert Michael Guillory; the author of the article is Bert Moore, Editor, AIM Global. This article is a good source for *Technological Issues*. As the article implies, it covers the possibility of counterfeiting RFID tags.

<http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=393&zoneid=24>

RFID Hacking Threat Overstated. No author for this article. This article is a good source for technical information for *Technological Issues*, covering encryption, security and spoofing.

<http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=292&zoneid=26>

RFID Security: Getting Serious. The author of this article is Bert Moore, Editor, RFID Connections, AIM Global. This article is a good source for Ramifications (business and ethical), covering cost vs. benefit; it is also a good source for *Technological Issues*, covering encryption, security and prototyping.

<http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=721&zoneid=43>

ACM Source (through ProQuest database)

The following source was obtained in the ACM Digital Library database through the ABI/Inform Global database on the UMUC Electronic Library; ABI/Inform Global uses ProQuest as its database search tool. A login to the UMUC Library Resources is required to review this article.

Untraceable RFID tags via insubvertible encryption. The authors of this paper are Giuseppe Ateniese, Johns Hopkins University, Jan Camenisch, IBM Research, and Breno de Medeiros, Florida State University. This paper introduces a new cryptographic primitive, called insubvertible encryption, which can be applied to RFID tags, providing strong protection against tracing. This paper is a good source for *Technological Issues*.

<http://delivery.acm.org.ezproxy.umuc.edu/10.1145/1110000/1102134/p92-ateniese.pdf?key1=1102134&key2=8707308411&coll=GUIDE&dl=ACM&CFID=71685867&CFTOKEN=87221014>

Excuse me, I'm having an Accelerando moment. This message was posted by Autopope on his own web page, and addresses the Dutch virus paper and includes comments. This message with comments is a good source for *Technological Issues* and *Ramifications* (business and ethical). <http://autopope.livejournal.com/115429.html>

Silicon.com Sources

Silicon.com is a business technology website, with the emphasis on business. I found 3 articles on this site which applied to this research paper. They are in chronological order according to date of publication.

E-crime and hacking – RFID viruses? Don't panic. The author of this article is Jo Best, a freelance writer. This article is about the proof-of-concept virus created by Dutch researchers. This article is a good source for *Technological Issues*.

<http://www.silcon.com/research/specialreports/ecrime/0,3800011283,39157280,00.htm>

E-crime and hacking – RFID ‘not safe from DoS attacks’. The author of this article is Tom Espiner, a writer for ZDNet UK. This article is about RFID standards and security, and is a good source for *Technological Issues*.

<http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39158120,00.htm>

Concerns about wireless tracking devices discussed. The author of this article is Winter Casey, a writer for National Journal’s Technology Daily. This article covers government and business use of RFID and associated security and privacy concerns, and is a good source for *Technological Issues*. <http://www.govexec.com/dailyfed/0306/032206tdpm1.htm>

Viruses Worm Their Way Into RFID Technology. The author of this article is Raj Dash, and is a good source for *Technological Issues*. <http://technopedia.info/tech/2006/05/18/viruses-worm-their-way-into-rfid-technology.html>

A Hacker’s Guide to RFID. The author of this article is Arik Hesseldahl, of Forbes.com. This article covers security of RFID tags, although it does provide a link to a program called RFDump designed by Lukas Grunwald, a German consultant and speaker at the Black Hat Security Briefings conference in Las Vegas, Nevada, on July 29, 2004. It is a good source for *Technological Issues*.

http://www.forbes.com/business/commerce/2004/0729/cx_ah_0729rfid.html

The Real RFID Security Issue. The author of this article is Eric Lundquist, a writer for eWeek; this article is actually in 2 parts with the same title. The article covers security issues with RFID technology, and is a good source for *Technological Issues*.

<http://www.eweek.com/article2/0,1759,1941421,00.asp> and

<http://www.eweek.com/article2/0,1895,1941432,00.asp>

‘Mr. RFID’ Discusses RFID Security. The author of this article is Eric Lundquist, a writer for eWeek. The article is a partial interview with Kevin Ashton, VP of ThingMagic and a co-founder of MIT’s Auto-ID Center, and is a good source for *Technological Issues*.

<http://www.eweek.com/article2/0,1759,1941977,00.asp>

Dutch Researchers Create RFID Malware. The author of this article is Ryan Naraine, a writer for eWeek. This article perpetuates the RFID virus claim by Rieback, Crispo and Tanenbaum, and is a good source for *Technological Issues*.

<http://www.eweek.com/article2/0,1895,1938391,00.asp>

The RFID Hacking Underground. The author of this article is Annalee Newitz, a contributing editor for Wired Magazine. This article presents examples of RFID hacking actually accomplished, and is a good source for *Technological Issues*.

http://www.wired.com/wired/archive/14.05/rfid_pr.html

HOWTO make an RFID virus. This article was posted to [boingboing.net](http://www.boingboing.net) by David Pescovitz. This posting contains some quotes from Ben Giddings of ThingMagic that counters the Dutch researchers' claims, and is a good source for *Technological Issues*.

http://www.boingboing.net/2006/03/16/howto_make_an_rfid_v.html

Is Your Cat Infected with a Computer Virus? The authors of this [controversial] paper are Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, researchers at the Vrije Universiteit Amsterdam. This paper is a proof-of-concept of a self-replicating virus, and is a good source for *Technological Issues* and because this paper spawned a lot of discussion is a good source for *Technological Issues*. <http://www.rfidvirus.org/>

Schneier on Security. The author of this message is Bruce Schneier, a security technologist and author. This message elaborates on the Dutch virus paper in technical detail, and is a very good source for *Technological Issues*.

http://www.schneier.com/blog/archives/2006/03/rfid_chips_and_1.html

Verichip RFID Implant Hacked! This article was a CASPIAN press release, covering RFID security issues and their implications for Verichip's IPO. This article is a good source for *Technological Issues*. <http://www.sypchips.com/press-releases/verichip-hacked.html>.

Meanwhile, back in Arphidland. The author of this message is Bruce Sterling, a science fiction writer; he also prepared the Foreword for the "Spychips" book by Albrecht & McIntyre. This message elaborates on the Dutch virus paper, and is a good source for *Technological Issues*. http://wiredblogs.tripod.com/sterling/index.blog?entry_id=1440029

Virus Allegations Rock RFID World. This blog was posted by Laurie Sullivan, and is about the Dutch researchers' "RFID virus", and is a good source for *Technological Issues*. http://techsearch.cmp.com/blog/archives/2006/03/melanie_rieback.html?loc=software

As part of an information system, even the lowly RFID tag is vulnerable. The author of this article is David Talbot. This article is an interview with Daniel Engels at the Auto-ID Labs at MIT, and counters the virus threat proposed by the Dutch researchers. This article is a good source for *Technological Issues*.

http://www.technologyreview.com/read_article.aspx?id=16797&ch=infotech

How To Infect An Airport. The author of this message is Jeremy Wagstaff, a technology columnist for The Wall Street Journal and BBC. This message elaborates on the Dutch virus paper, and is a good source for *Technological Issues*.

http://www.loosewireblog.com/2006/03/how_to_infect_a.html

Ramifications

Medical

Couple Implants Microchips Into Hands. No author for this article, but published under Good Morning America on ABC News web site. This article is about 2 different people who voluntarily had microchips implanted into their hands, and is a good source for *Ramifications* (medical and legal).

<http://abcnews.go.com/GMA/Technology/story?id=1699462&page=1> and
<http://abcnews.go.com/GMA/Technology/story?id=1699462&page=2>

AIM Global Source

AIM Global is the industry association and worldwide authority on automatic identification and mobility technologies. AIM members are providers and users of technologies, systems, and services that capture, manage, and integrate accurate data into larger information systems. There are more than 900 members in 43 countries.

A Book Review of “Spychips: How major corporations and government plan to track your every move with RFID.” The author of the article is Bert Moore, Editor, AIM Global; the authors of the book are Katherine Albrecht and Liz McIntyre, with a Foreword by Bruce Sterling of Wired.com. This article is a rich source for *Ramifications* (medical, legal and religious).

<http://www.aimglobal.org/members/news/templates/aimpress.asp?articleid=478&zoneid=1>

Are you ready to “Get Chipped”? The author of this message posting is Sterling D. Allan. This posting is about an article in Time Magazine by Lev Grossman, and is about technology moving faster than legislation. This posting is a good source for *Ramifications* (medical, legal and business). http://groups.yahoo.com/group/davids_outcasts/message/12466

Harvard Medical CIO’s RFID Chip. The author of this article is David M. Ewalt, a Forbes writer. This article is about John Halamka, a CIO and physician, and his reaction to the RFID chip embedded in his arm, and is a good source for *Technological Issues* and *Ramifications* (medical and business).

http://www.forbes.com/technology/2005/03/03/cx_de_0303toiyboxhalamka.html?partner=rss

Doctor tagged with RFID worries about privacy. No author for this article. This article revisits the previous article 4 months earlier, with the CIO now worried about privacy of his data on the RFID chip. This article is a good source for *Ramifications* (medical, legal and business).

<http://www.e-health.insider.com/news/item.cfm?ID=1349>

FDA approves computer chip for humans. No author for this MSNBC article. The article is about how RFID devices could help doctors with stored medical information, and is a good source for *RFID Basics* (uses), *Technological Issues* and *Ramifications* (medical and legal). <http://msnbc.msn.com/id/6237364/>

Oilempire.us Sources: This web site is a veritable smorgasbord for RFID stories and comments, and is a very good source for *Ramifications* (medical, political, legal, business, and religious). There are several sources used from this web site that are listed elsewhere in this review and are listed separately in the References. <http://www.oilempire.us/rfid.html>

ProQuest Sources

The following sources were obtained through the ABI/Inform Global database on the UMUC Electronic Library; ABI/Inform Global uses ProQuest as its database search tool, and parentheses are used for identification in the References. These sources are in chronological order according to date of publication, and the document URL is included at the end of each source review. A login to the UMUC Library Resources is required to review these articles.

Embedded Microelectronic Chip Enhances RFID Tracking. The author of this article is Doreen R. Coppola, writer for Pharmaceutical Technology. This article is about enhanced RFID for medical use and for improved security, and is a good source for *Ramifications* (medical and business). <http://ezproxy.umuc.edu/login?url=http://proquest.umi.com.ezproxy.umuc.edu/pqdweb?did=618930891&sid=1&Fmt=4&clientId=8724&RQT=309&VName=PQD>

Turning a prophet. The author of this article is Joseph Conn, a writer for Modern Healthcare. This article is about a physician, John Halamka, CareGroup CIO, having a RFID chip embedded in his right arm. This article is a good source for *Ramifications* (medical and business). <http://ezproxy.umuc.edu/login?url=http://proquest.umi.com.ezproxy.umuc.edu/pqdweb?did=804795851&sid=3&Fmt=3&clientId=8724&RQT=309&VName=PQD>

RFID Journal Source

RFID Journal is the premiere source of literature for Radio Frequency Identification-related information, issues, analysis, opinions and links; however, it is not the only source of literature for RFID.

An RFID Code of Conduct. The author of this article is Lisa J. Sotto, a guest writer for RFID Journal. The article references statutory and medical issues for medical use of RFID. This article is a good source for *Ramifications* (medical, legal and business). <http://www.rfidjournal.com/article/articleview/1624/1/133/>

FDA Letter Raises Questions About Verichip Safety, Data Security. This article was a CASPIAN press release; it also incorporated a CASPIAN special report on RFID devices. It is a good source for *Ramifications* (medical, business and legal). <http://www.spsychips.com/press-releases/verichip-fda.html> (w/special report at <http://www.spsychips.com/devices/verichip-fda-report.html>)

Business

ACM Sources (through ProQuest database)

The following sources were obtained in the ACM Digital Library database through the ABI/Inform Global database on the UMUC Electronic Library; ABI/Inform Global uses ProQuest as its database search tool. These sources are in chronological order according to date of publication, and the document URL is included at the end of each source review. A login to the UMUC Library Resources is required to review these articles.

Me and My Shadow. The author of this article is Aaron Weiss, a technology writer and Web developer in upstate New York. This article is about the tradeoff between privacy and efficiency, and is a good source for *Ramifications* (business and legal). <http://delivery.acm.org.ezproxy.umuc.edu/10.1145/950000/940832/p24-weiss.pdf?key1=940832&key2=8566308411&coll=GUIDE&dl=ACM&CFID=71685867&CFTOKEN=87221014>

The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. The authors of this paper are Ari Juels, Ronald L. Rivest, and Michael Szydlo. This paper proposes the use of “selective blocking” by “blocker tags” as a way of protecting consumers from unwanted scanning of RFID tags attached to items they may be carrying or wearing. This paper is a very good source for *Ramifications* (business and legal). <http://delivery.acm.org.ezproxy.umuc.edu/10.1145/950000/948126/p103-juels.pdf?key1=948126&key2=2945308411&coll=GUIDE&dl=ACM&CFID=71685867&CFTOKEN=87221014>

A Prototype on RFID and Sensor Networks for Elder Healthcare: Progress Report. The authors of this paper are Loc Ho, Venturi Wireless, Melody Moh and Zachary Walker, San Jose University, and Takeo Hamada and Ching-Fong Su, Fujitsu Laboratories of America. This paper covers an in-home elder healthcare system that monitors patients’ medication intake, and is a good source for *Ramifications* (business, medical and legal). <http://delivery.acm.org.ezproxy.umuc.edu/10.1145/1090000/1080164/p70-ho.pdf?key1=1080164&key2=8542308411&coll=GUIDE&dl=ACM&CFID=71685867&CFTOKEN=87221014>

AIM Global Sources

AIM Global is the industry association and worldwide authority on automatic identification and mobility technologies. AIM members are providers and users of technologies, systems, and services that capture, manage, and integrate accurate data into larger information systems. There are more than 900 members in 43 countries.

RFID and Homeland Permeability. The author of this article is Bert Moore, Editor, AIM Global. This article is a good source for *Ramifications* (political, business, and legal), covering U.S. travel documents and business transacted across the U.S. borders; it is a somewhat useful source for *Ramifications* (business).

<http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=1142&zoneid=43>

Guest Editorial: Privacy Invasion as ROI. The author of this article is Ross Stapleton-Gray, Ph.D., Stapleton-Gray & Associates, Inc., and the director of the Sorting Door project (<http://www.sortingdoor.com>), an examination of RFID, surveillance and privacy issues. This article is a good source for *Ramifications* (business and legal).

<http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=427&zoneid=24>

RFID Tags in Human Beings. The author of this article is Kamla Bhatt. The article is about an Ohio company that embedded RFID chips in 2 employees, and is a good source for *Ramifications* (business and medical).

<http://kamlabhatt.wordpress.com/2006/02/13/rfid-tags-in-human-beings/>

RFID's High Cost Deters Businesses. The author of this article is Renee Boucher Ferguson, a writer for eWeek. This article addresses the business issues with RFID, and is a good source for *Ramifications* (business).

<http://www.eweek.com/article2/0,1895,1934328,00.asp>

The RFID Imperative. The author of this article is Meridith Levinson, a Senior Writer for CIO Magazine and so-called expert shopper. This article is about the business ramifications of RFID, and is a good source for *Technological Issues* and *Ramifications* (business, legal and ethical). The article contains comments by other technology consultants and a sidebar on privacy which is a good source for *Ramifications* (business and legal).

<http://www.cio.com/archive/120103/retail.htm> and

http://www.cio.com/archive/120103/retail_sidebar_2.html

Perspective: RFID Tags: Big Brother in Small Packages. The author of this article is Declan McCullagh, CNET News.com's chief political consultant. This article is about tracking objects that are worn, eaten or carried, and is a good source for *Ramifications* (business and legal). <http://news.com/2010-1069-980325.html>

Injectable chip opens door to ‘human bar code’. The author of this article is Charles J. Murray. This article is about the new chips by VeriChip and their impact, and is a good source for *Ramifications* (business, legal and medical). <http://www.oilempire.us/rfid.html>

ProQuest Source

The following source was obtained through the ABI/Inform Global database on the UMUC Electronic Library; ABI/Inform Global uses ProQuest as its database search tool, and parentheses are used for identification in the References. A login to the UMUC Library Resources is required to review this article.

The pros and cons of RFID. This article has no author and is found in Strategic Direction. The title explains what the article is about and is a good source for *Ramifications* (business and legal).

<http://ezproxy.umuc.edu/login?url=http://proquest.umi.com.ezproxy.umuc.edu/pqdweb?did=851354071&sid=3&Fmt=4&clientId=8724&RQT=309&VName=PQD>

RFID: No Human Tracking. No author for this article. This article is about RFID industry best practices, and is a good source for *Ramifications* (business). <http://www.redherring.com/Article.aspx?a=16703&hed=RFID%3A+No+Human+Tracking>

RFID Journal Sources

RFID Journal is the premiere source of literature for Radio Frequency Identification-related information, issues, analysis, opinions and links; however, it is not the only source of literature for RFID. These reviews are in chronological order according to date of publication.

The Privacy Nightmare. The author of this article is Mark Roberti, founder and Editor of RFID Journal. This article is an opinion on why the author thinks that only an aggressive PR campaign and an “enforceable” code of ethics will get people to accept self-regulation of RFID tracking of consumer products. Even though the opinion was written in 2002, it still applies to the current situation surrounding RFID tracking. This article was very useful for *Ramifications* (business). <http://www.rfidjournal.com/article/view/144/1/1/>

Faith in the System, Part II. The author of this article is Mark Roberti, founder and Editor of RFID Journal. This article is an opinion on why the capitalist system that some privacy advocates think will exploit consumers will, in fact, protect them. This article is a good source for *Ramifications* (business and legal). <http://www.rfidjournal.com/article/articleview/1011/1/2/>

Standards Progress – It’s All Relative. The author of this article is Chris Martins, a guest writer for RFID Journal. The article pertains to the perceived slow pace of RFID standards, and is a good source for *Ramifications* (business, political and legal).
<http://www.rfidjournal.com/article/articleview/1674/1/128/>

FTC Asks RFID Users to Self-Regulate. The author of this article is Jonathan Collins, a writer for RFID Journal. This article, as the title implies, is about the FTC stating that companies should bear responsibility for addressing privacy concerns raised by RFID applications. The article is eerily reminiscent of the article written by Mark Roberti in 2002 – The Privacy Nightmare, when he stated that self-regulation would only be accepted if there was an aggressive PR campaign and an “enforceable” code of ethics. This article is a good source for *Ramifications* (business, political and legal).
<http://www.rfidjournal.com/article/articleview/1437/1/132/>

Don’t Get Behind the Regulatory Eight Ball. The author of this article is Ronald E. Quirk, Jr., a guest writer for RFID Journal. The article is written more for businesses than individuals, but it covers current government regulations on RFID. The article is a good source for *Ramifications* (business and legal).
<http://www.rfidjournal.com/article/articleview/1484/1/133/>

The Consequences of Convenience. The author of this article is Mary Catherine O’Connor, Associate Editor of RFID Journal. The article is an opinion on how whether the convenience of RFID will strengthen or weaken privacy protections. The article is a good source for *Ramifications* (business and legal).
<http://www.rfidjournal.com/article/articleprint/2067/-1/1>

Political

AIM Global Sources

AIM Global is the industry association and worldwide authority on automatic identification and mobility technologies. AIM members are providers and users of technologies, systems, and services that capture, manage, and integrate accurate data into larger information systems. There are more than 900 members in 43 countries. These reviews are in chronological order according to date of publication.

Editorial: RFID Legislation—Protection or Pause Button? No author for this article. This article is a good source for *Ramifications* (political and legal).
<http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=433&zoneid=24>

Editorial: 2006 -- the Year of RFID Legislation? The author of this article is Bert Moore, Director, Communications & Media Relations, AIM Global. The name is misleading on this article, as it only covers the legislation being introduced in New Hampshire (with a hint of pending legislation in California); however, it does lay out the wording in the proposed bill, which most likely will be used by other states to craft their legislation. It is a good source for *Ramifications* (political and legal).

<http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=586&zoneid=43>

Which is Better: RFID Legislation or RFID Guidelines? The author of this article is Bert Moore, Editor, RFID Connections, AIM Global. This article addresses the legislation in California and answers the question, "What does legislation accomplish?" This is a good source for *Ramifications* (political and legal).

<http://www.aimglobal.org/members/news/templates/aimsights.asp?articleid=667&zoneid=43>

RFID: For the Common Good. The author of this article is Dan Mullen, President, AIM Global. This article is a good source for *Technological Issues*, covering security and types of RFID used. It is a somewhat useful source for *Ramifications* (political), with a good point on what might have not happened had certain legislation been passed based on incomplete and slanted information.

<http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=1204&zoneid=24>

Bill would prohibit mandatory microchip implants. The author of this article is Ryan J. Foley, an Associated Press writer. The article is about Wisconsin becoming the first state to ban governments and private businesses from forcing microchip implants. This article is a good source for *Ramifications* (political, legal and business).

<http://www.duluthsuperior.com/mld/duluthsuperior/14418898.htm>

RFID Journal Source

RFID Journal is the premiere source of literature for Radio Frequency Identification-related information, issues, analysis, opinions and links; however, it is not the only source of literature for RFID.

The Law of the Land. The author of this article is Mark Roberti, founder and Editor of RFID Journal. This article is an opinion on how legislation introduced in Utah and California will force companies in the U.S. to address the privacy issue. Even though this opinion was written in 2004, it still applies to the current privacy issue situation surrounding RFID technology. This article is a good source for *Ramifications* (political and legal).

<http://www.rfidjournal.com/article/articleview/811/>

Spychips.com Sources

Spychips.com is a site created by CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering). The group's founder, Katherine Albrecht, is a

noted and respected national privacy advocate. They are in chronological order according to date of publication.

RFID Implants: Fine For Thee, But Not For Me. This article was a CASPIAN press release, covering the reluctance of Tommy Thompson to get “chipped” as promised. This article is a good source for *Ramifications* (political).

<http://www.spychips.com/press-releases/verichip-thompson-no-implant.html>.

Homeland Security RFI Heightens Public Concerns Over RFID. This article was a CASPIAN press release covering use of RFID to track moving cars at 55 miles per hour. This article is a good source for *Ramifications* (political and legal).

<http://www.spychips.com/press-releases/dhs-rfid.html>.

Legal

ACM Source (through ProQuest database)

The following source was obtained in the ACM Digital Library database through the ABI/Inform Global database on the UMUC Electronic Library; ABI/Inform Global uses ProQuest as its database search tool. A login to the UMUC Library Resources is required to review this article.

RFID Is X-Ray Vision. The author of this article is Frank Stajano, Associate Professor at the University of Cambridge, Cambridge, UK. This article about the technical difficulties of protecting privacy in a world saturated with RFID tags. This article is a good source for *Technological Issues* and *Ramifications* (legal and business).

<http://delivery.acm.org.ezproxy.umuc.edu/10.1145/1090000/1082015/p31-stajano.pdf?key1=1082015&key2=5063308411&coll=GUIDE&dl=ACM&CFID=71685867&CFTOKEN=87221014>

AIM Global Sources

AIM Global is the industry association and worldwide authority on automatic identification and mobility technologies. AIM members are providers and users of technologies, systems, and services that capture, manage, and integrate accurate data into larger information systems. There are more than 900 members in 43 countries. These reviews are in chronological order according to date of publication.

RFID and Privacy Laws. No author for this article. This article is a good source for *Ramifications* (legal); it also raises a legal issue about cloned tags and prosecution.

<http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=311&zoneid=24>

Editorial: “Privacy” vs. Safety. No author for this article. This article is a good source for *Ramifications* (legal), as it covers a tradeoff between personal privacy and safety (and security).

<http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=338&zoneid=24>

AIM Global Publishes RFID Position Statement on Consumer Privacy and Security. No author for this article. This article is a good source for *Ramifications* (legal and political). One questionable term – unbiased – in the fifth paragraph relating to AIM Global’s position to deliver information on auto ID technologies; AIM Global represents the manufacturing and marketing side of RFID, not the consumers or Government.

<http://www.aimglobal.org/members/news/templates/aimpress.asp?articleid=459&zoneid=1>

VeriChip: RFID Microchip Implants for Humans. The author of this article is Uri Dowbenko, the author of “Bushwacked: Inside Stories of True Conspiracy”. This article is about the potential uses of RFID chips and privacy issues, and is a good source for *RFID Basics* (potential uses), *Technological Issues* and *Ramifications* (legal, political, medical and business).

<http://www.conspiracyplanet.com/channel.cfm?channelid=74&contentid=900&page=1>

New-look passports. No author for this article from The Economist. This article is about the problems with the new RFID-chipped passports, and is a good source for *Ramifications* (legal and business).

http://www.economist.com/science/displayStory.cfm?story_id=3666171

FDA approves implanted RFID chip for humans. This message was posted by Hannibal on artstechnica.com, and covers privacy issues with RFID. This message is a good source for *Ramifications* (legal, business and medical).

<http://arstechnica.com/news.ars/post/20041013-4305.html>

When Small Technology is a Big Deal: Legal Issues Arising From Business Use of RFID. The author of this paper is D. Zachary Hostetter, a student at the Shidler School of Law at the University of Washington, and is a good source for *Ramifications* (legal and business). <http://www.lctjournal.washington.edu/Vol2/a010Hostetter.html>

Perspective: RFID Tags: The People Say No. The author of this article is Michael Kanellos, editor at large for CNET News. This article is about fear of RFID technology, and is a good source for *Ramifications* (legal and business).

http://news.com.com/RFID+tags:+The+people+say+no/2010-1039_3-5332468.html

RFID tagging humans. This message was posted by Aristotle on kurzweilai.net and it includes over 20 comments. This message is a good source for *Ramifications* (legal, medical and religious). http://www.kurzweilai.net/mindx/show_thread.php?rootID=46432

RFID Position Statement of Consumer Privacy and Civil Liberties Organizations. This statement was posted on the Privacy Rights Clearinghouse web site, and was issued by 8 privacy rights organizations and endorsed by 37 others. This statement addresses how RFID technology can threaten privacy and civil liberties and contains other RFID Position Papers as attachments, and is a very good source for *Ramifications* (legal and business). <http://www.privacyrights.org/ar/RFIDposition.htm>

Why the 'Real ID' Act is a real mess. The author of this article is Anita Ramasastry, a FindLaw columnist. This article is about the Real ID Act and its effects on privacy, and is a good source for *Ramifications* (legal, political and business). <http://www.cnn.com/2005/LAW/08/12/ramasastry.ids/index.html>

RFID Journal Source

RFID Journal is the premiere source of literature for Radio Frequency Identification-related information, issues, analysis, opinions and links; however, it is not the only source of literature for RFID.

RFID, Electronic Eavesdropping and the Law. The authors of this article are Reuven R. Levary, Professor of Decision Sciences, Cook School of Business, David Thompson, Kristen Kot and Julie Brothers, all three completing joint JD/MBA degrees at Saint Louis University. This article covers 2 federal laws in depth (Electronic Communication Privacy Act and The Wiretap Act) and discusses legal ramifications of these acts as it applies to RFID use in the business world; it also has links to 2 other sources used in this research paper from the Organization for Economic Cooperation and Development (OECD) and the Federal Trade Commission (FTC). The article is a rich source of information for *Ramifications* (legal, political and business). <http://www.rfidjournal.com/article/articleview/1401/1/133/>

Religious

RFID Foes Find Righteous Ally. The author of this article is Mark Baard, and is about the religious beliefs of Katherine Albrecht and her anti-RFID crusade. This article is a good source for *Ramifications* (religious). <http://www.wired.com/news/privacy/1,68133-0.html>

Group Fears RFID Chips Could Herald 'Mark of the Beast'. The author of this article is Jim Brown of AgapePress. This article is about a Christian group that opposes the use of RFID technology, and is a good source for *Ramifications* (religious and legal). http://news.christiansunite.com/Religion_News/religion02480.shtml

From MicroChips to the Mark of the Beast. The author of this article is Thomas Horn (news with view.com). This article is about the various uses of RFID chips up to 2005 and the religious implications of such use. The article is a good source for *Ramifications* (religious). <http://www.conspiracyplanet.com/channel.cfm?channelid=74&contentid=3346>

Oilempire.us Sources: This web site is a veritable smorgasbord for RFID stories and comments, and is a very good source for *Ramifications* (medical, political, legal, business, and religious). There are several sources used from this web site that are listed elsewhere in this review and are listed separately in the References. <http://www.oilempire.us/rfid.html>

RFID and religion. The author of this posting is Alex Soojung-Kim Pang, and is a good source for *Ramifications* (religious). http://future.iftf.org/2005/07/rfid_and_religi.html

US issues first RFID passports. This article was posted by Marc Pertion and has 35 comments, and is a good source for *Ramifications* (religious, political and legal). <http://www.engadget.com/2006/03/13/us-issues-first-rfid-passports/>

RFIDs of the Beast, starring Katherine Albrecht. The author of this posting is David Pescovitz of boingboing.net, and is a good source for *Ramifications* (religious). http://www.boingboing.net/2005/07/14/rfids_of_the_beast_s.html

Summary of Literature Reviewed

The sources of literature reviewed for this study include major news outlets, technology websites and journals, technology companies, consolidated federal and civilian law databases, educational journals, websites and databases, and personal websites and blogs. A major drawback of the major news outlets is that they will pull a story off of their Web Site without a retraction; CNN.com did this to two articles about the Dutch researchers who allegedly put a virus in a RFID tag. It could mean one of two things when major news outlets pull articles off of their Web Sites – either the information in the article is untrue, or the article drew too much criticism. A lot of the literature is from the major players in RFID technology and privacy issues/legislation, and as such it is a major strength of the literature reviewed. In addition, several of the sources refer to other sources within this research paper, which allow for smoother and stronger arguments. However, a lot of the discussion by these major players involves opinions, which also makes it a major limitation of the literature used in this study. Even though this limitation exists, the opinions by the sources in this study should not be discounted, as they lend themselves well to the statement this study is formulated to address.

Research Hypothesis

It is the intention of the United States government to control everyone using RFID technology.

CHAPTER THREE METHODOLOGY

Design

Review of literature from multiple sources – major news outlets, technology web sites and journals, library databases and message-hosting web sites.

Procedures

Categorize sources and separate relevant information into compartments within the sections (RFID Basics, Technological Issues and Ramifications).

Assumptions & Limitations

The experts identified are indeed recognized experts in their field and that they are not self-titled experts. Limitation – not enough quantitative sources to back up claims (mostly conjecture and opinion).

CHAPTER FIVE

ANALYSIS AND DISCUSSION

Most of the problems associated with RFID technology stems from a lack of understanding, not only from current and potential end-users, but also from the technology and business industry. To overcome this problem, this paper will cover the basics of RFID, some technological issues surrounding using the technology in humans, and the ramifications of using this technology in humans.

Radio Frequency Identification Basics

Definition of Radio Frequency Identification

RFID is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders [including chips; all 3 hereafter referred to as tags]. An RFID tag is a small object that can be attached to or incorporated into a product, animal, or person. RFID tags contain silicon chips and antennas to enable them to receive and respond to radio frequency queries from an RFID transceiver. Passive tags require no internal power source, whereas active tags require a power source. (Wikipedia, 2006)

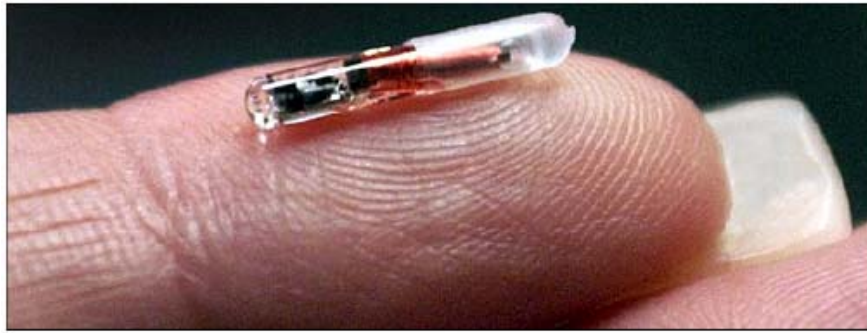
History of Radio Frequency Identification

The technology used in RFID has been around since the early 1920's. The British, in 1939, invented a similar technology (though not really RFID technology) called IFF, which was used by the allies in World War II to identify airplanes as friend or foe. In 1945, Leon Theremin invented an espionage tool for the Soviet government which retransmitted incident radio waves with audio information. Even though this device was a passive covert listening device, not an identification tag, it has been attributed as the first known device and a predecessor of RFID technology. (Wikipedia, 2006)

Another early work exploring RFID is the landmark 1948 paper by Harry Stockman, titled "Communication by Means of Reflected Power" (Proceedings of the IRE, pp 1196-1204, October 1948). Stockman predicted that "...considerable research and development work has to be done before the remaining basic problems in reflected-power communication are solved, and before the field of useful applications is explored." (Wikipedia, 2006)

Mario Cardullo claims that his U.S. Patent 3,713,148 (<http://patft.uspto.gov/netacgi/nph-Parser?patentnumber=3,713,148>) in 1973 was the first true ancestor of modern RFID – a passive radio transponder with memory. (<http://www.rfidjournal.com/article/articleview/392/1/2/>) The first demonstration of today's reflected power (backscatter) RFID tags was done at the Los Alamos Scientific Laboratory in 1973 (http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf). (Wikipedia, 2006)

In 2004, the U.S. FDA approved the use of RFID tags that can be implanted in humans, tags created by VeriChip Corporation, a subsidiary of Applied Digital Solutions Incorporated (see Figure 1). (Wikipedia, 2006; Gilbert, 2004) This approval caused a spike in privacy advocates' claims of potential misuse by the government and individuals' claims that RFID technology was "The Mark of the Beast" (which has unfortunately been attributed to Social Security numbers and bar codes as well).



Agence France-Presse

Figure 1 – Human Implantable Chip (Agence France-Presse, 2004)

As of this date, the RFID tags are used for prescription tracking and usage, SCM, livestock management, access control for vehicles and persons, remote data collection, and location sensing. Future potential uses have been proposed for automatic POS systems for cashier-less store checkouts, individual product tracking from manufacture to sale, and low-cost remote sensor systems for weather, road conditions and noise level monitoring. (Wikipedia, 2006)

Types of Radio Frequency Identification Tags/Chips

There are three types of tags in current usage – passive, semi-passive (also known as semi-active), and active. These various types can be found in Figure 2.

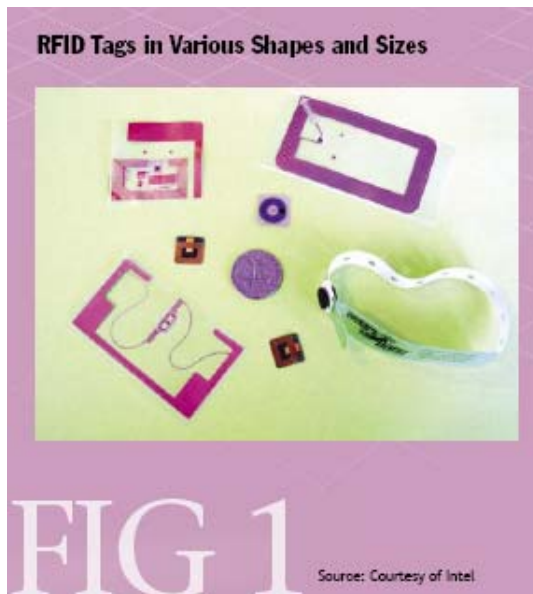


Figure 2 – RFID Tags in Various Shapes and Sizes (Want, 2004)

Passive RFID Tags

Passive RFID tags have no internal power supply. The minute electrical current induced in the antenna by the incoming radio frequency signal from the transponder (or reader) provides just enough power for the CMOS integrated circuit (IC) in the tag to power up and transmit a response. Most passive tags signal by backscattering the carrier signal from the reader. This means that the antenna has to be designed to both collect power from the incoming signal and also to transmit the outbound backscatter signal. The response of a passive RFID tag is not just an ID number; it can also contain nonvolatile EEPROM for storing data. The lack of an onboard power supply means that the device can be quite small, and as of 2006, the smallest such devices measured 0.15 mm x 0.15 mm, and are thinner than a sheet of paper (7.5 micrometers). The addition of the antenna creates a tag that varies from the size of a postage stamp to the size of a postcard. Passive tags have practical read distances ranging from about 2 mm up to a few meters depending on the chosen radio frequency and antenna design/size. Due to their simplicity in design they are also suitable for manufacture with a printing process for the antennas. Passive RFID tags do not require batteries, and can be much smaller and have an unlimited life span. Non-silicon tags made from polymer semiconductors are currently being developed by several companies globally. (Wikipedia, 2006)

Because passive tags are cheaper to manufacture and have no battery, the majority of RFID tags in existence are of the passive variety. In 2005, the lowest cost EPC tag available on the market was 7.2 cents each in volumes of 10 million units or more. On May 1, 2006, SmartCode announced the first ever \$0.05 tag. The nickel tag has been the holy grail that was originally calculated by the Auto-ID Center (now EPCglobal) as the tag price that will bring RFID to the masses. The price is only for the inlay (chip and antenna only) and does not include

the label (adhesive, etc.) which already exists on most products today. In large scale deployments companies are also starting to embed these inlays directly into the products themselves or the packaging without the need for a paper label (WalMart, Proctor & Gamble, pharmaceutical companies, and Department of Defense contractors). The nickel price is good for orders of 100 million or more, which is an extremely large number for most of us, but not for large commercial producers and pharmaceutical companies which ship billions of products each year. (Wikipedia, 2006)

Semi-Passive RFID Tags

Semi-passive RFID tags are very similar to passive tags except for the addition of a small battery. This battery allows the tag IC to be constantly powered, which removes the need for the antenna to be designed to collect power from the incoming signal. Antennas can therefore be optimized for the backscattering signal. Semi-passive RFID tags are thus faster in response. (Wikipedia, 2006)

Active RFID Tags

Unlike passive and semi-passive RFID tags (response tags), active RFID tags have their own internal power source which is used to power any ICs that generate the outgoing signal. Active RFID tags are typically beacon tags but are also available as response tags. Beacon tags are often called beacon or broadcast because they transmit their tag data and ID at a predetermined fixed interval. Some active RFID tags also have advanced features such as temperature logging which have been used in concrete maturity monitoring or to monitor the temperature of perishable goods (see Figure 3 below). Active RFID tags may have a longer range and larger memories than passive or semi-passive tags, as well as the ability to store additional information sent by the transceiver. To economize power consumption, many beacon tags operate at fixed intervals. At present, the smallest active tags are about the size of a coin. Many active tags have practical ranges of tens of meters and battery life of up to 5 years. (Wikipedia, 2006)



Figure 3 – Temperature Sensing RFID Tag (Want, 2004)

Radio Frequency Identification System

An RFID system may consist of several components: Tags, tag readers, edge servers, middleware, and application software. The purpose of an RFID system is to enable data to be transmitted by a mobile device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc. The use of RFID in tracking and access applications first appeared during the 1980s. RFID quickly gained attention because of its ability to track moving objects. As the technology is refined, more pervasive and possibly invasive uses for RFID tags are in the works. (Wikipedia, 2006)

In a typical RFID system, individual objects are equipped with a small, inexpensive tag. The tag contains a transponder with a digital memory chip that is given a unique electronic product code. The interrogator, an antenna packaged with a transceiver and decoder, emits a signal activating the RFID tag so it can read and write data to it. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's IC (silicon chip) and the data is passed to the host computer. The application software on the host processes the data, often employing Physical Markup Language (PML). (Wikipedia, 2006)

Take the example of books in a library. Security gates can detect whether or not a book has been properly checked out of the library. When users return items, the security bit is re-set and the item record in the Integrated Library System is automatically updated. In some RFID solutions a return receipt can be generated. At this point, materials can be roughly sorted into bins by the return equipment. Inventory wands provide a finer detail of sorting. This tool can be used to put books into shelf-ready order (see Figure 4 below). (Wikipedia, 2006)



Figure 4 - RFID Tags Used in Libraries: Square book tag, round CD/DVD tag and rectangular VHS tag. (Wikipedia, 2006)

Radio Frequency Identification Usage

Current uses of RFID technology by commercial business and government are as follows (Wikipedia, 2006):

- Talking Prescriptions – 13.56 MHz tags are being placed on prescriptions for Visually Impaired Veterans. The Department of Veterans Affairs Outpatient pharmacies are now supplying the tags with label information stored inside that can be read by a battery powered, talking prescription reader. This reader speaks information such as drug name, instructions, warnings, etc. (<http://www.envisionamerica.com/scriptalk.htm>).

- High-frequency RFID tags are used in library book or bookstore tracking, pallet tracking, building access control, airline baggage tracking, and apparel and pharmaceutical item tracking. High-frequency tags are widely used in identification badges, replacing earlier magnetic stripe cards. These badges need only be held within a certain distance of the reader to authenticate the holder. The American Express Blue credit card now includes a high-frequency RFID tag.
- UHF RFID tags are commonly used commercially in case, pallet, and shipping container tracking, and truck and trailer tracking in shipping yards.
- Microwave RFID tags are used in long range access control for vehicles.
- RFID tags are used for electronic toll collection at toll booths with Georgia's Cruise Card, California's FasTrak, Illinois' I-Pass, the expanding eastern states' E-ZPass system, Florida's SunPass, Massachusetts's Fast Lane, North Texas NTTA and Houston HCTRA EZ Tag. The tags are read remotely as vehicles pass through the booths, and tag information is used to debit the toll from a prepaid account. The system helps to speed traffic through toll plazas as it records the date, time, and billing data for the RFID vehicle tag.
- Sensors such as seismic sensors may be read using RFID transceivers, greatly simplifying remote data collection.
- In January 2003, Michelin began testing RFID transponders embedded into tires. After a testing period that is expected to last 18 months, the manufacturer will offer RFID-enabled tires to car makers. Their primary purpose is tire-tracking in compliance with the United States Transportation, Recall, Enhancement, Accountability and Documentation Act (TREAD Act).
- Some smart cards embedded with RFID chips are used as electronic cash, such as the SmarTrip card in Washington, DC, to pay fares in mass transit systems and/or retail outlets. The Chicago Transit Authority recently began using RFID technology in their Chicago Card.
- Starting with the 2004 model year, a *Smart Key/Smart Start* option became available to the Toyota Prius. Since then, Toyota has been introducing the feature on various models around the world under both the Toyota and Lexus brands, including the Toyota Avalon (2005 model year), Toyota Camry (2007 model year), and the Lexus GS (2006 model year). The key uses an active RFID circuit which allows the car to acknowledge the key's presence within approximately 3 feet of the sensor. The driver can open the doors and start the car while the key remains in a purse or pocket.
- In August 2004, the Ohio Department of Rehabilitation and Correction (ODRH) approved a \$415,000 contract to evaluate the personnel tracking technology of Alanco

Technologies. Inmates will wear wristwatch-sized transmitters that can detect if prisoners have been trying to remove them and send an alert to prison computers. This project is not the first such rollout of tracking chips in US prisons. Facilities in Michigan, California and Illinois already employ the technology.

- During the 2006 NASCAR racing season, the Goodyear Tire and Rubber Company began testing RFID tags by Advanced ID Corporation (<http://www.advancedidcorp.com/>) embedded in racing tires. It is expected that these tags will be commercially available by the end of 2006.

Potential Usage

RFID tags are often envisioned as a replacement for UPC barcodes, having a number of important advantages over the older barcode technology. They may not ever completely replace barcodes, due in part to their higher cost and in other part to the advantage of more than one independent data source on the same object. The new EPC, along with several other schemes, is widely available at reasonable cost. (Wikipedia, 2006)

The storage of data associated with tracking items will require many terabytes on all levels. The escape is filtering, as nobody will save data without defined purpose. It is likely that goods will be tracked preferably by the pallet using RFID tags, and at package level with UPC from unique barcodes. (Wikipedia, 2006)

The unique identity in any case is a mandatory requirement for RFID tags, despite special choice of the numbering scheme. RFID tag data capacity is big enough that any tag will have a unique code, while current bar codes are limited to a single type code for all instances of a particular product. The uniqueness of RFID tags means that a product may be individually tracked as it moves from location to location, finally ending up in the consumer's hands. This may help companies to combat theft and other forms of product loss. Moreover, the tracing back of products is an important feature that gets well supported with RFID tags containing not just a unique identity of the tag but also the serial number of the object. This may help companies to cope with quality deficiencies and resulting recall campaigns, but also contributes to concern over post-sale tracking and profiling of consumers. (Wikipedia, 2006)

It has also been proposed to use RFID for POS store checkout to replace the cashier with an automatic system which needs no barcode scanning. However this is not likely to be possible without a significant reduction in the cost of current tags and changes in the operational process around POS. There is some research taking place, however, this is some years from reaching fruition. (Wikipedia, 2006)

Active RFID tags also have the potential to function as low-cost remote sensors that broadcast telemetry back to a base station. Applications could include sensing of road conditions by implanted beacons, weather reports, and noise level monitoring. (Wikipedia, 2006)

Standards

There is no global public body that governs the frequencies used for RFID. In principle, every country can set its own rules for this. The main bodies governing frequency allocation for RFID in the United States is the FCC. Low-frequency (LF: 125 - 134.2 kHz and 140 - 148.5 kHz) and high-frequency (HF: 13.56 MHz) RFID tags can be used globally without a license. Ultra-high-frequency (UHF: 868 MHz-928 MHz) cannot be used globally as there is no single global standard. In North America, UHF can be used unlicensed for 908 - 928 MHz, but restrictions exist for transmission power. The North American UHF standard is not accepted in France as it interferes with its military bands. These frequencies are known as the ISM bands (Industrial Scientific and Medical bands). The return signal of the tag may still cause interference for other radio users. (Wikipedia, 2006)

Some standards that have been made regarding RFID technology include (Wikipedia, 2006):

- ISO 11784 & 11785 - These standards regulate the Radio frequency identification of animals in regards to Code Structure and Technical concept.
- ISO 14223/1 - Radio frequency identification of Animals, advanced transponders - Air interface.
- ISO 10536
- ISO 14443
- ISO 15693
- ISO 18000
- EPCglobal - this is the standardization framework that is most likely to undergo International Standardization according to ISO rules as with all sound standards in the world, unless residing with limited scope, as customs regulations, air-traffic regulations and others. Currently the big distributors and governmental customers are pushing EPC heavily as a standard well accepted in their community, but not yet regarded as for salvation to the rest of the world.

GS1 and GS1 US operate the joint venture EPCglobal. EPCglobal is working on international standards for the use of RFID and the EPC in the identification of any item in the supply chain for companies worldwide. The organization's board of governors includes representatives from GS1, GS1 US, The Gillette Company, Procter & Gamble, Wal-Mart, Hewlett-Packard, Johnson & Johnson, Checkpoint Systems and Auto-ID Labs and others. (Wikipedia, 2006)

The EPCglobal gen 2 standard was approved in December 2004, and is likely to form the backbone of RFID tag standards moving forward. This was approved after a contention from Intermec that the standard may infringe a number of their RFID related patents. It was decided that the standard itself did not infringe their patents, but it may be necessary to pay royalties to Intermec if the tag were to be read in a particular manner. EPC Gen2 is short for EPCglobal UHF Generation 2. EPC standardization is headed to become adopted by ISO, e.g. in

accordance with complementary standardization based on the ISO standard 18000-6. (Wikipedia, 2006; Borck, 2006)

A primary security concern surrounding RFID technology is the illicit tracking of RFID tags. Tags which are world-readable pose a risk to both personal location privacy and corporate/military security. Such concerns have been raised with respect to the United States Department of Defense's recent adoption of RFID tags for supply chain management. More generally, privacy organizations have expressed concerns in the context of ongoing efforts to embed EPC RFID tags in consumer products. (Wikipedia, 2006)

A second class of defense uses cryptography to prevent tag cloning. Some tags use a form of "rolling code" scheme, wherein the tag identifier information changes after each scan, thus reducing the usefulness of observed responses. More sophisticated devices engage in challenge-response protocols where the tag interacts with the reader. In these protocols, secret tag information is never sent over the insecure communication channel between tag and reader. Rather, the reader issues a challenge to the tag, which responds with a result computed using a cryptographic circuit keyed with some secret value. Such protocols may be based on symmetric or public key cryptography. Cryptographically-enabled tags typically have dramatically higher cost and power requirements than simpler equivalents, and as a result, deployment of these tags is much more limited. This cost/power limitation has led some manufacturers to implement cryptographic tags using substantially weakened, or proprietary encryption schemes, which do not necessarily resist sophisticated attack. For example, the Exxon-Mobil Speedpass uses a cryptographically-enabled tag manufactured by Texas Instruments, called the Digital Signature Transponder (DST), which incorporates a weak, proprietary encryption scheme to perform a challenge-response protocol. (Wikipedia, 2006)

Still other cryptographic protocols attempt to achieve privacy against unauthorized readers, though these protocols are largely in the research stage. One major challenge in securing RFID tags is a shortage of computational resources within the tag. Standard cryptographic techniques require more resources than are available in most low cost RFID devices. RSA Security has patented a prototype device that locally jams RFID signals by interrupting a standard collision avoidance protocol, allowing the user to prevent identification if desired. Various policy measures have also been proposed, such as marking RFID tagged objects with an industry standard label. (Wikipedia, 2006)

Technological Issues

Performance

Passive RFID tags that operate at frequencies up to 100 MHz are usually powered by magnetic induction, the same principle that drives the operation of household transformers. An alternating current in the reader coil induces a current in the tag's antenna coil, allowing charge to be stored in a capacitor, which then can be used to power the tag electronics. Information in

the tag is sent back to the reader by loading the tag's coil in a changing pattern over time, which affects the current being drawn by the reader coil – a process called *load modulation*. To recover the identity of the tag, the reader simply decodes the change in current as a varying potential developed across a series resistance. Unlike a transformer, the coils of a reader and a tag are separated in space, and coupling between the coils can occur only where the magnetic field lines of the reader coil intersect with the tag coil, the *near field* region (see Figure 5 below). (Want, 2004)

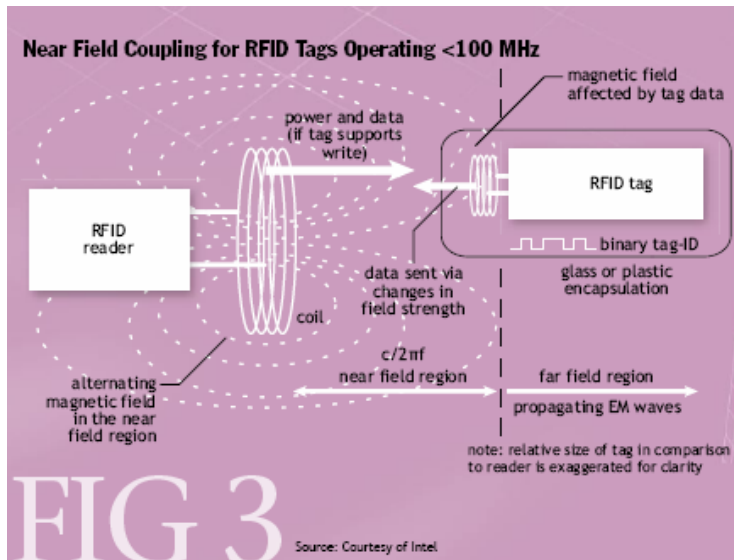


Figure 5 – RFID Near Field Communication (Want, 2004)

Beyond this distance the energy breaks away from the antenna as propagating waves called a radio signal; this is known as the *far field* region. The boundary of the near field and far field is governed by the frequency of the alternating current and is approximately limited to the distance of $c/2\pi f$; for example, at 13.56 MHz used by the ISO 15693 and 14443 standards, this distance is 3.6 meters, but at 915 MHz, used by EPCglobal, the range of the reader if based on near field coupling would be limited to six centimeters, reducing its usefulness. Note that even at the lower frequency it is not guaranteed a reader/tag pair will be able to exchange data up to the $c/2\pi f$ distance. Unfortunately, the magnetic field strength also falls off fairly rapidly, proportional to a $1/d^3$ factor, where d is the distance from the center of the reader coil to the tag. If the field strength is too weak at a given distance, it will not be possible to provide the tag with the energy it needs to switch on. This effect can be mitigated by increasing the size of the reader coil and the tag coil, but for handheld readers and tags attached to small objects, there are obvious limitations. In practice, at 13.56 MHz, most systems operate with a range between 1 and 30 centimeters, considerably shorter than the near field limit. To circumvent the range problem at higher frequencies above 100 MHz – namely, *electromagnetic capture*. This technique involves the use of electromagnetic waves that propagate from the antenna in the far field region to power the tag. A high-frequency tag operates much as an old-fashioned crystal-set radio, which requires no battery because it is able to capture enough energy from the received signal.

Because the tag is operating beyond the near field, however, data cannot be sent back to the reader using load modulation; instead, radio frequency backscatter must be used: The tag electronics changes the impedance of the antenna, reflecting back some of the incident RF energy to the reader (see Figure 6 below). The reader, using a sensitive receiver, decodes the ID of the tag from the pattern of reflections, expressed as a varying amplitude in the received signal. For far field communication, the energy delivered to the tag follows an inverse square law, and the return signal another inverse square law. Thus, the transmit power is attenuated by a $1/d^4$ law even before considering operational inefficiencies, where d is the separation of the tag and reader – a very rapid decline indeed, but the system can be made to work over a distance of three to four meters. (Want, 2004)

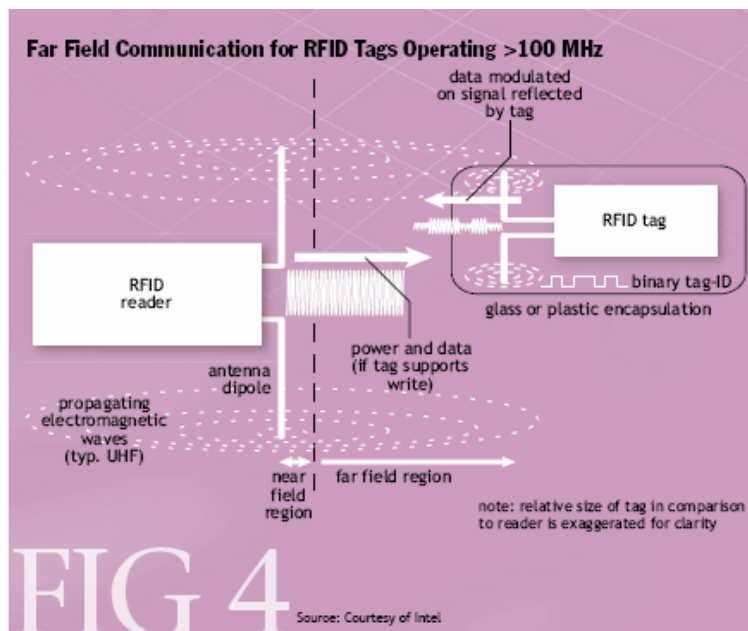


Figure 6 – RFID Far Field Communication (Want, 2004)

Modern high-frequency tags, like the microprocessors in PCs, are beneficiaries of Moore's law. The laws of physics dictate the amount of energy that a reader can transmit to an RFID tag. The amount of energy required to power a digital circuit clocking at a particular frequency, however, has been falling annually as a result of advances in silicon technology that have led to the regular reduction in the size of the lithographic features in integrated circuits. Thus, every few years, RFID systems can be designed with greater read range, since the tags consume less power when clocked at the same frequency. In recent years, RFID tag functionality has also become more sophisticated. Today's tags can accommodate a larger number of bits in the ID code than earlier models could, enabling the creation of billions of tags with unique IDs (EPCglobal specifies tags with 96-bit codes representing 79 billion billion (octillion) numbers, although some are redundant because of the inclusion of a checksum code). RFID readers have also been improved by the development of inexpensive receivers that are capable of detecting the tiny signals a battery-less UHF tag can return, which at distances of three meters registers power levels on the order of a billionth of a milliwatt. (Want, 2004)

Orientation: Although RFID does not require line of sight to operate, the reader cannot communicate effectively with a tag that is oriented perpendicular to the reader antenna. If a number of objects with RFID tags attached are placed in a random orientation, some will be oriented in a direction that makes them invisible to the reader. Since the tagged object cannot be re-oriented, the solution to this problem is to vary the position of the reader or build advanced antennas that are less sensitive to orientation. One approach is to use many readers that have a diversity of orientations relative to the read area and to sequence through them performing multiple scans from different directions. The read results can then be merged, providing a much greater chance of identifying all of the tags present. Another solution employs antenna diversity by using a single reader with several switchable antennas that can be sequentially connected to the reader. This is likely to be a more cost-effective solution because it would reduce the number of relatively expensive radio and processing components needed to build the system. (Want, 2004)

Reader Coordination: Most RFID readers are not designed to operate in the presence of another reader that is also scanning for tags. To date, this has not been a significant problem, as RFID has been in limited deployment without much opportunity for readers to interfere with each other. As electronic tags become more common, however, readers will be deployed on a larger scale, effectively garbling the data for systems in proximity of each other. This problem will become particularly serious if many mobile hand-readers are in use within close range of each other. (Want, 2004)

Signal Processing: Noise interfering with the signal is another problem. Application of advanced data-coding techniques in the tag electronics may also improve noise immunity and allow some multitag signal collisions to be separated and interpreted correctly. This may require more costly signal processing in the reader, but the benefits of greater accuracy will eventually lead to acceptance by a larger market. (Want, 2004)

Material Independence: Disruption of RFID signals by the makeup of objects themselves – whether products or humans – can be an issue. Because tags use tuned RF circuits to receive interrogation signals, it is possible to detune or attenuate the signals if placed next to metallic packaging or objects (see Figure 7 below for an example of RFID use in packaging designed to avoid this problem). This problem is a challenging one, as the most obvious solution is to change the packaging material in products or the type of materials inserted into humans, but clearly some products and bio-materials do not have alternatives, particularly where robustness and airtight storage is required for products and where strength and durability is required for humans. (Want, 2004) Currently, there are commercial products for sale that are designed to thwart automatic invasive RFID readers from reading your RFID-enabled products (see Figure 8 and Figure 9 below); something simple as a metallic armband can be used to block the unauthorized reading of tags in/on humans.

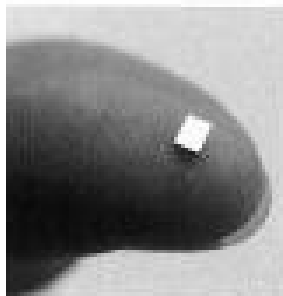
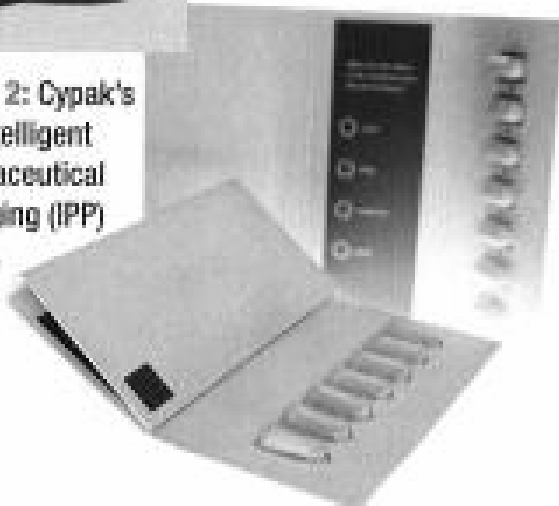


Figure 1: Cypak's microelectronic sensor chip is about 0.3 mm in height and can store 32 kilobytes of memory.

Figure 2: Cypak's first Intelligent Pharmaceutical Packaging (IPP) design.



rlcs

n/a

Figure 7 – RFID CYPAC Chip, Commercial – In Use Today (Coppola, 2004)



Figure 8 – RFID Blocking Wallet (<http://www.difrwear.com/products.shtml>)



Figure 9 – RFID Blocking Passport Case (<http://www.difrwear.com/products.shtml>)

Longer Range: In practice, most of the lower-frequency RFID systems can read tags at a maximum distance of about meter, and the UHF systems extend that to three to four meters. Some companies are claiming that more than five meters is possible, although this may be under very ideal conditions, high sensitivity to orientation, and possibly with a tag battery assist or energy harvesting. As the power requirements of the silicon in a tag drop and the semiconductor industry designs more sensitive receivers at reasonable cost, reliable longer-range systems should become possible and expand the usefulness of RFID in warehouses and other voluminous environments. (Want, 2004)

Security

Just as with other technologies, there are vulnerabilities with RFID technology, too. The three major vulnerabilities with RFID technology this paper will cover are Viruses (and other types of attacks), Hacking (product and identity theft), and Tracking Misuse. Even though tracking of individuals with RFID is more of an ethical issue, it is discussed here because of its security issues and potential for misuse due to these security issues by individuals, corporations and various government agencies.

Viruses (and other attacks)

The idea of viruses in RFID technology has crossed people's minds before, and has been discussed within the RFID manufacturing community for many years. In a recent study by scientists from the Computer Systems Group at the Vrije Universiteit in Amsterdam – Is Your Cat Infected with a Computer Virus? (Rieback, et al, 2006) – they revealed that data from RFID tags can be used to exploit back-end software systems. This paper also introduced a proof-of-concept virus, which uses the track and trace tags to compromise middleware systems using a SQL injection attack. This type of attack was reviewed by many experts in the auto-ID field, and many of them were quick to dismiss the impact of this type of attack in the wild. (Best, 2006)

Ben Giddings of ThingMagic, says “The RFID Virus is absolutely laughable... This is so laughably stupid, but somehow it got picked up by the news outlets because it contains buzzwords: “RFID” and “Virus”. Really, what they're doing is the equivalent of: 1. Designing a barcode system to automatically self-destruct if it ever reads a barcode of 1337 1337, for no reason other than to prove it's dangerous. 2. Broadcasting to the world that the barcode system will self-destruct if it ever reads a barcode of 1337 1337. 3. Intentionally reading a barcode of 1337 1337. 4. Claiming that barcodes are dangerous.” (Pescovitz, 2006) What they did was create their own system with known security problems, create their own software to exploit the security problems they created, and then extrapolate their findings to the entire RFID industry. This type of virus attack is already in the wild – it infects the back-end software that runs the system, not the tags themselves.

Graham Cluley, Senior Technology Consultant for antivirus company Sophos, chimed in with “Of course, any device that can store data can store virus code as well. But that does not mean that the virus would be able to spread or be in any way effective.” (Best, 2006) The scientists themselves stated there are problems with the virus, including the fact that it will be easily spotted by a database administrator. They state that “developers of the wide variety of RFID-enhanced systems will need to “armour” their systems, to limit the damage that is caused once hackers start experimenting with RFID exploits, RFID worms and RFID viruses on a larger scale.” (Rieback et al, 2006)

Kevin Ashton, Vice President of Marketing at ThingMagic, a co-founder of MIT’s Auto-ID Center, and prior Associate Director at Proctor and Gamble, echoes most of the other experts’ statements about the “Virus paper”: “That was just a piece of rubbish, frankly. They treated data as it was code, which no one would do. It would be like driving a car with a blindfold and then concluding that all cars were unsafe.” (Lundquist, 2006)

Since viruses are currently a non-issue with RFID right now, one can sit back and not worry about any attacks, right? Wrong! RFID is just as vulnerable to DoS attacks as other network systems; but just how vulnerable could it be? Well, researchers at Edith Cowan University in Perth, Australia, found that Gen2 tags can be disrupted by overloading the readers with data. (Espiner, 2006) Isn’t that a problem? The answer to this is not really. These researchers demonstrated that from a range of one meter they could disrupt communications between tags and readers, putting the tag into a communication fault-state; however, to get that close to a reader with equipment that could send a data overload would be the same as some of the stunts in “Mission: Impossible.” One would have to be seen carrying the equipment around, and even if one could get close enough to send the data he or she would immediately be identified as an outsider. This would be a good story line for CSI, though.

Hacking (product and identity theft)

Identity theft has become a big issue lately, with the emergence of the “paperless” society the U.S. government is so conveniently pushing. But how could identity theft be a problem with RFID? According to security researcher Jonathan Westhues, it is relatively simple to clone a VeriChip implanted in a person’s arm and program a new chip with the same number. (Spychips, 2006) The only problem with this type of cloning is that someone would have to get within a few inches of the intended target and also have the necessary RFID equipment (to include proprietary software) to “hijack” the signals from RFID-enabled objects. (Newitz, 2006) It is possible to accomplish this type of identity theft, but the cost of the equipment needed for this type of theft to occur is cost-prohibitive at this point for criminals.

Product theft is entirely a different ballgame. The potential for this type of theft is much higher than identity theft because the cost-benefit ratio is much higher. Lukas Grunwald, a German security consultant, co-wrote a free program called RFDump that allows him to re-write the data on tags that are not “locked. (Newitz, 2006; Hesseldahl, 2006) Imagine being able to

re-write the price of a \$500 bottle of champagne to \$5 (and get away with it); is this something that one could consciously carry out? It's been said that the fraud possibilities alone are mind-boggling – imagine a pallet-load of 20 high-end servers getting reprogrammed to present itself as soap powder. The only problem with this scenario is that someone would have to destroy the tag and replace it, and hope that the cashier (or warehouse person) didn't catch the discrepancy; there is no real way to overwrite data unless its not locked when its initially written (this is another security problem, but it can be fixed by enforced security policies). (Talbot, 2006) There are many examples around the world of tags that were not locked down (mostly because they were being used to test whether the RFID system worked or not), and again these examples are extrapolated to the entire RFID industry by privacy advocates trying to further their own agenda.

However, according to Yossie Oren, a researcher at the Weizmann Institute in Israel, "Companies who use tags must not assume that the data they read from the tags was not put there by somebody else. Just like when writing Web applications, one would have to assume any input from the outside world may contain malicious or corrupted data." (Lundquist, 2006) So it behooves RFID hardware manufacturers (who are typically the software vendor as well) to do background checks on hardware and software developers. On the other hand, with the growth of RFID-based smartcards and touchless/contactless payment systems, there might eventually be enough motivation for criminals to devise methods of RFID-based fraud. (Dash, 2006)

Tracking Misuse

The U.S. government is currently issuing RFID-enabled passports to track their own citizens, and are requiring other countries to issue their citizens RFID-enabled passports before they are allowed into the U.S. (causing many European countries to clamp down on travel by U.S. citizens by making it tougher to enter or exit their countries). To address privacy concerns with these passports, the U.S. government added technology to them to prevent the inappropriate "skimming" of passport data by other technology in the vicinity. (Casey, 2006) One way around the issue of unauthorized access to data on RFID-enabled objects is to make the tag untraceable using what three researchers did using Insubvertible Encryption in the tags so only authorized readers could access the data. (Ateniesse et al, 2005) The only issue with this is that the U.S. government would be able to obtain the equipment needed to access data from any manufacturer via the Patriot Act, and they would be the only one's who could technically track every item (or person) with an RFID tag. The only positive is that marketers would not be able to track every object (or person) with an RFID tag such as in the movie "Minority Report."

RFID security is everyone's issue, and RFID manufacturers are well aware of the risks associated with this technology. Most of the problems associated with RFID are perceived by those with little knowledge of what this technology can do. Kevin Ashton, Vice President of Marketing for ThingMagic summed it up best when he said, "The most important aspect of RFID security is to implement security practices that already exist for other kinds of network technology. Ninety-nine percent of security concerns in RFID can be addressed by existing technology. They are solved problems." (Lundquist), 2006) So, security is not really an issue in

using RFID technology in humans. But why would the U.S. government want to use this technology to keep track of us anyway? This question will be answered in the following section – Ramifications.

Ramifications

This is the part of the research paper in which there will be conjecture and speculation as to the outcome of using RFID technology in humans. The ramifications of using RFID technology in humans are broken up into 5 areas: Medical, Business, Political, Legal and Religious. All five areas will have ethical overtones, so the Ethical section which was originally in this paper was removed as being redundant.

Medical

Implanting RFID chips in paper is relatively easy; all someone would have to do is glue it to the paper or integrate the chip into the rolling process. Implanting the RFID chips into humans, however, takes a doctor; one just can't go to the local "Claire's" and have an "expert chipper" implant the chip.

The majority of humans to have RFID chips implanted are those that can't take care of themselves due to debilitating diseases (Alzheimer's, coma, etc.) and those that are non-living. The medical benefit of having these 2 classes of people is enormous, as those who cannot take care of themselves could be easily tracked down if they wander off, or the right medications could get to the right person if they could be scanned to see what their medical history says. The only drawback to this is that the personal data would be available to anyone with a scanner. To address this issue, Cypak (a Swedish pharmaceutical manufacturer) designed an electronic data capturing system aimed at monitoring patient activity more securely (see Figure 7). (Coppola, 2004) Also, the healthcare industry could institute an "RFID Code of Conduct" to protect medical data that is collected. (Sotto, 2005)

When the FDA approved the use of RFID chips in humans in 2004, they outlined some medical warnings with the chips: Adverse tissue reaction, migration of implanted transponder, compromised information security, failure of implanted transponder, failure of inserter, failure of electronic scanner, electromagnetic interference, electrical hazards, magnetic resonance imaging incompatibility, and needle stick. According to Katherine Albrecht, CASPIAN founder and director, MRI incompatibility is the biggest risk. (Spychips, 2004) In this she is correct; however, there is an MRI incompatibility risk associated with metallic plates in the body as well, which she deftly avoids in her retort. Also, there are risks associated with any medical procedure. Take a look at the warnings on a bottle of pain medicine. The risks of taking pain medicine are worse than the risks associated with having a chip implanted in one's arm. In response to Albrecht's book "Spychips: How major corporations and government plan to track your every move with RFID", AIMGlobal Editor Bert Moore counters by saying, "If this book had been published in 2003, some points that were raised might have been valid. The fact is,

however, many of the concerns expressed in the book have either been (or are being) addressed, and many of the scary “facts” have been shown to be highly overstated, not technically feasible, or just plain bad judgment on the part of some marketing concerns.” (Moore, 2005)

Business

Cost vs. Benefit

According to Weiss (2003):

What if a technology came along that decreased prices for consumers while maximizing profits for vendors? What if the applications of this technology ranged from streamlined inventory management to automated checkout, allowing you – among many other possibilities – to wave your cell phone in the air to make an instant, on-the-run purchase? But what if this same technology could be used to track your behavior and whereabouts long after you’ve left the store?

Would one take advantage of this technology for one’s convenience? And would anyone really care what is being purchased or where it’s located? Ross Stapleton-Gray, Ph.D., a business consultant, attempts to answer these questions by identifying Privacy Invasion as ROI. (Stapleton-Gray, 2004) In his paper, he references an essay by the Association for Automatic Identification and Mobility in 2004 entitled “The ROI of Privacy Invasion.” The essay established and demolished a strawman vision of potential government surveillance through RFID, positing that it would cost the U.S. government in excess of \$1 Trillion to establish a “national spy network” of RFID readers monitoring all of the malls, airports, parks, playgrounds and churches. Their verdict – that spending a Trillion dollars just to construct an RFID-based surveillance network wouldn’t show sufficient ROI – seems fairly obvious. So there won’t be a top-down creation of a national spy infrastructure; it will be bottom-up, being created by both the private sector and government a little at a time. Dr. Stapleton-Gray also references Metcalfe’s law as it should apply to RFID: RFID will increase in utility as a function of all of the tags and readers deployed by all parties, and not merely linearly. RFID’s “promiscuity” (especially with passive tags, where readers broadcast queries at any and all tags within range, and find what they’re looking for among all the tags which respond) is analogous to the “flat” Internet, where any node can reach out to any other. If the deployment of RFID follows an arc similar to what has occurred with the Internet, one should expect to see a proliferation of local systems, all useful in their primary applications, eventually knitted together into even more valuable systems of systems. Those interworked systems will find it easier to exchange information, and small pools of data will be merged and refined to produce larger and more valuable collections. And as with the Internet, open architectures and widely recognized standards, such as the 30-year-old standard for product identifiers established for the print bar code, will form a strong base upon which to build interesting new applications. There are serious potential consequences for personal privacy in a future RFID-pervasive world. Perhaps now is the time for everyone to

figure out how to build in more privacy protections in the future “Internet of things” and to anticipate what will become possible once the infrastructure is too pervasive and critical to live without. So, would someone take advantage of this technology for his or her own convenience? It only costs about \$200 to have one implanted.

One potential way of balancing privacy vs. convenience is using blocker tags – tags that can simulate many ordinary RFID tags simultaneously, thereby “blocking” RFID readers from reading the tags on (or in) your person. (Juels et al, 2003) Another potential way is to get people to accept self-regulation of RFID tracking by manufacturers, retailers and government. (Roberti, 2002)

Political

Legislation and Regulations

Current legislation in individual states is as follows (Wikipedia, 2006; Moore, 2006; Foley, 2006):

California – SB1834; PURPOSE: Restrict the way businesses and libraries in California use RFID tags attached to consumer products or using an RFID reader that could be used to identify an individual. Defeated by members of the California state assembly on June 25, 2005.

Massachusetts – HB 1447, SB 181; PURPOSE: Requires labels regarding use and purpose of RFID on consumer products; requires the ability to remove tags; and restricts info on tags to inventory and like purposes.

Maryland – HB 354; PURPOSE: Creates a task force to study privacy and other issues related to RFID and report on whether legislation is needed.

Missouri – SB 128; PURPOSE: Requires a conspicuous label on consumer packaging with RFID disclosing existence of the tag and that the tag can transmit a unique ID before and after purchase.

Nevada – AB 264; PURPOSE: Requires manufacturers, retailers and others to ensure placement of a label regarding existence of RFID on product prior to sale.

New Hampshire – HB 203; PURPOSE: Requires written or verbal notice of existence of a tracking device on any product prior to sale.

New Mexico – HB 215; PURPOSE: Requires businesses purveying tagged items to post notices on their premises and labels on the products; requires removal or deactivation of tag at point of sale.

Rhode Island – H 5929; PURPOSE: Prohibits state or local government from using RFID to track movement or identity of employees, students or clients or others as a condition of a benefit or service.

South Dakota – HB 1114; PURPOSE: Prohibits requiring a person to receive implant of an RFID chip.

Tennessee – HB 300, SB 699; PURPOSE: Requires conspicuous labeling of goods containing RFID disclosing existence of RFID and that it can transmit unique information.

Texas – HB 2953; PURPOSE: Prohibits school district from requiring student to use an RFID device for identification; requires school to provide alternative method to those who object to RFID.

Utah – HB 185; PURPOSE: Amends computer crime law to include RFID.

Wisconsin – Assembly Bill 291; PURPOSE: Prohibits anyone, including employers or government agencies, from requiring people to have microchips implanted in them. Violators would face fines of up to \$10,000.

Demagoguery

According to Mullen (2006):

Suppose, 15 years ago, you had been told about a technology that could potentially erase (or copy) all the files from your computer, aid criminals in stealing your credit card and bank information, and even make you a party to unethical and illegal activities. And suppose a state legislature proposed banning that technology. Would you have supported the legislation? Or suppose that you had been told that there was a new technology on the horizon that would claim one life every 13 minutes in the U.S. alone, damage the environment, and leave the country hostage to foreign interests. Would you have supported banning that technology? Couched in these terms, many people would. Yet if such legislation had been enacted, neither the Internet nor the automobile would be in use today.

A lot of people are trying to portray RFID technology in much the same way. Many reports, and now many political debates, focus only on the negative scenarios without providing an accurate perspective on how the technology works and how it is improving and protecting our quality of life. The question is, does one ban the technology or establish realistic

and effective safety and security procedures (best practices) to protect users of the technology? Fortunately, it appears that many legislatures are leaning toward the latter in the bills they are bringing forth; however, unfortunately, many news organizations and privacy advocates are still striving for the prior option when it comes to RFID technology.

Legal

Border Security

The primary use of RFID at the borders is to speed up processing for everyone trying to cross (people and vehicles), not National Security. This technology could be used to rapidly identify who and what was coming across the border at any point in time, and could aid in the protection of our borders as well.

Electronics-Related Laws

The Electronic Communication Privacy Act most likely will be amended to cover some of the privacy concerns with RFID technology. This act already outlaws wiretapping and other forms of electronic eavesdropping, possession of wiretapping or electronic eavesdropping equipment, and use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping. In essence, this act prohibits any person from intentionally intercepting, or endeavoring to intercept wire, oral or electronic communications by using an electronic, mechanical or other device unless that conduct is specifically authorized or expressly not covered (much like the current warrantless wiretapping that the U.S. government is currently doing). (Levary et al, 2005)

The Wiretap Act sets the stage for accessing information and the ramifications of doing so. It defines what constitutes a criminal act and stipulates punishment by imprisonment or fine. In some instances, for an act to be deemed criminal, a person performing that act must demonstrate both criminal intent and action. (Levary et al, 2005)

Civil Liberties

“Hypothetically, law enforcement agencies or even private security companies will be able to track where you’ve been, with whom you associate and what you own with this technology. Imagine a semi-retired senior citizen in a rented maroon blazer knowing everything about your day. It is the fear most often raised that the technology will enable governments to keep tabs on everyone.” (Kanellos, 2004) According to Harold Davis of Syracuse, New York, “I couldn’t help but notice that one of the most effective uses for the RFID tags on humans was in a prison setting – which is exactly what society in general would become, if this particular technology were mandated somehow.” (Kanellos, 2004) The U.S. Department of Homeland Security is intent on obtaining technology that can even read government-issued documents from up to 25 feet away, pinpoint pedestrians on the street, and glean the identity of people whizzing

by in cars at 55 miles per hour. (Spychips, 2006) Combined with the Patriot Act, would anyone be able to do anything unscrupulous without the government knowing it, much like the movie “The Matrix”?

RFID may be an effective tool in criminal investigations. It is conceivable that an RFID chip could be used to identify the original purchaser of an item found at a crime scene. The technology could also be used to identify someone in a crowd. Crime scene investigators might find RFID useful for keeping track of the evidence collected from crime scenes. While this technology appears promising, however, it is not foolproof. Malfunctions happen in any technology, and tags can be transferred and/or counterfeited. Relying on RFID technology alone for prosecution is a Pandora’s box that should not be opened. (Levary et al, 2005)

Religious

Mark of the Beast, or the End of the World?

There is a wide-spread belief among Christians in the U.S. that human RFID tags are a demonic tool. Several ardent bloggers have pointed out that in the Bible, Revelations 13:16-17 reads: “and he causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads. And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name.” (Kanellos, 2004) Unfortunately, these same remarks were said about the UPC symbols and Social Security Numbers. But “with a bible-thumper in the White House, and the popular success of the Left Behind series or Christian-themed novels, American culture may be ready to hear Albrecht’s message that RFID tags, such as the rather bizarre VeriChip implant, may become the must-have gadget for any servant of Satan.” (Baard, 2005) According to Tim Miller, professor of religious studies at the University of Kansas, “There may be lots and lots of preaching, but as long as the bargains are there, any boycott will not likely have much adverse effect.” (Baard, 2005)

Several bloggers also stated, “Wow, you want us to go one worse then the Nazis?” and “Tracking implants are not for a free society, they are for a prison state.” (Kurzweil, 2005) OilEmpire states that RFID chips are “a technological advancement over Nazi tattooing of prisoners.” Also, according to John Connor, a spokesman for “The Resistance of Christ,” “... what its [sic] going to do is it’s going to turn every single one of us into a piece of inventory – not a human being – a piece of inventory, a number.” (Brown, 2005)

CHAPTER SIX

CONCLUSIONS AND RECOMMENDATIONS

While conducting research for this paper, I found it odd that there was an utter lack of participation by U.S. citizens in using RFID technology. There are maybe a dozen people voluntarily “sporting” an RFID chip in their arm or hands, and out of those dozen people, 8 of them are concerned about the security of their personal data. Even the main proponent of having the chip implanted – the director of Health and Human Services – decided to not go through with it due to security concerns. However, RFID is a technology that can provide considerable value in a world in which operating costs are often dominated by labor time. The technical issues associated with RFID are likely to be resolved as further investments are made in the technology. The next major hurdle is not directly related to RFID technology itself (and does not deal with privacy), but the software systems that will be needed to manage RFID-based controls. The extensive use of electronic tagging technology will generate a flow of information that will be several orders of magnitude greater than it is now. Database management software (and those trained in managing them), will need to deal with item-level references, track individual objects for medical or safety purposes, respond to data recovered from a tag’s writable memory, and make automatic decisions about objects in particular environments. Many of these processes will need to operate in real-time, and systems that encompass all of these capabilities do not exist today; however, in 30 years or so they may exist, and even though the government has not had to fund the RFID infrastructure, they are in a position to utilize it to their benefit. So remember what the U.S. government is telling everyone without actually coming out and saying it – your call [and your person] may be monitored for quality control.

REFERENCES

- ACLU of northern California press release redistributed by the Electronic Frontier Foundation – Parents and civil liberties groups urge school district to terminate use of tracking devices.* (2005, February 8). Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- AIM global publishes RFID position statement on consumer privacy and security.* (2005, October 6). Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/aimpress.asp?articleid=459&zoneid=1>
- Albrecht, K. (2002). RFID: Tracking everything, everywhere. *Denver University Law Review*, Summer 2002, 79, 534-539 & 558-565. Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- Allan, S. (2002, March 9). (Time Magazine) Are you ready to “get chipped”? [Msg 12466]. Message posted to http://groups.yahoo.com/group/davids_outcasts/message/12466
- Aristotle. (2005, August 30). RFID tagging humans [Msg 46432]. Message posted to http://www.kurzweilai.net/mindx/show_thread.php?rootID=46432
- Ateniese, G., et al (2005, November 7). Untraceable RFID tags via insubvertible encryption. *Communications of the ACM*, 92-101. Retrieved May 19, 2006, from the ACM Digital Library database.
- Autopope (2006, March 15). Excuse me, I’m having an Accelerando moment [Msg 115429]. Message posted to <http://autopope.livejournal.com/115429.html>
- Baard, M. (2005, July 17). *RFID foes find a righteous ally.* Retrieved May 19, 2006, from <http://www.wired.com/news/privacy/1,68133-0.html>
- Best, J. (2006, March 16). *E-crime and hacking – RFID viruses? Don’t panic.* Retrieved May 20, 2006, from <http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39157280,00.htm>
- Bhatt, K. (2006, February 13). *RFID tags in human beings.* Retrieved April 6, 2006, from <http://kamlabhatter.wordpress.com/2006/02/13/rfid-tags-in-human-beings/>
- Borck, J. (2006, April 13). *Next-gen RFID tools expand the market – New standards, software help rf-enable business of any size.* Retrieved May 19, 2006, from http://www6.infoworld.com/products/print_friendly.jsp?link=/article/06/04/13/77019_16F_Erfidsoft_1.html

- Borck, J. (2006, April 13). *The long road to RFID interoperability – The gen2 standard means vendors and customers finally have a common platform*. Retrieved May 19, 2006, from http://www6.infoworld.com/products/print_friendly.jsp?link=/article/06/04/13/77022_16F%20Erfdsoftgen2_1.html
- Brown, J. (2005, March 29). *Group fears RFID chips could herald ‘mark of the beast’*. Retrieved May 19, 2006, from http://news.christiansunite.com/Religion_News/religion02480.shtml
- Casey, W. (2006, March 22). *Concerns about wireless tracking devices discussed*. Retrieved May 19, 2006, from <http://www.govexec.com/dailyfed/0306/032206tdpml.htm>
- Collins, J. (2005, March 10). *FTC asks RFID users to self-regulate*. *RFID Journal*. Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/articleview/1437/1/132/>
- Conn, J. (2005, February 28). *Turning a prophet*. *Modern Healthcare*, 35(9), 48-49. Retrieved May 19, 2006, from ABI/Inform Global (ProQuest) database.
- Coppola, D. (2004, April). *Embedded microelectronic chip enhances RFID tracking*. *Pharmaceutical Technology*, 28(4), 18-19. Retrieved May 19, 2006, from ABI/Inform Global (ProQuest) database.
- Couple implants microchips into hands*. (2006, March 8). Retrieved May 13, 2006, from <http://abcnews.go.com/GMA/Technology/story?id=1699462&page=1>
- Dash, R. (2006, May 18). *Viruses worm their way into RFID technology*. Retrieved May 19, 2006, from <http://technopedia.info/tech/2006/05/18/viruses-worm-their-way-into-rfid-technology.html>
- Doctor tagged with RFID worries about privacy*. (2005, July 29). Retrieved May 13, 2006, from <http://www.e-health-insider.com/news/item.cfm?ID=1349>
- Dowbenko, U. (2005). *VeriChip: RFID microchip implants for humans*. Retrieved May 19, 2006, from <http://www.conspiracyplanet.com/channel.cfm?channelid=74&contentid=900&page=1>
- Editorial: “Privacy” vs. safety*. (2005, April 26). Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=338&zoneid=24>
- Editorial: RFID legislation – protection or pause button?* (2005, August 29). Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=433&zoneid=24>

- Espiner, T. (2006, April 18). *E-crime and hacking – RFID “not safe from DoS attacks”*. Retrieved May 20, 2006, from <http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39158120,00.htm>
- Ewalt, D. (2005, March 3). *Harvard medical CIO’s RFID chip*. Retrieved May 13, 2006, from http://www.forbes.com/technology/2005/03/03/cx_de_0303toyboxhalamka.html?partner=rss
- FDA approves computer chip for humans*. (2004, October 13). Retrieved May 13, 2006, from <http://msnbc.msn.com/id/6237364>
- FDA letter raises questions about VeriChip safety, data security*. (2004, October 19). Retrieved May 13, 2006, from <http://www.spychips.com/devices/verichip-fda-report.html> and <http://www.spychips.com/press-releases/verichip-fda.html>
- Ferguson, R. (2006, March 6). *RFID’s high cost deters businesses*. Retrieved May 19, 2006, from <http://www.eweek.com/article2/0,1895,1934328,00.asp>
- Foley, R. (2006, April 15). *Bill would prohibit mandatory microchip implants*. *Duluth Superior*. Retrieved May 19, 2006, from <http://www.duluthsuperior.com/mld/duluthsuperior/14418898.htm>
- Gilbert, A. (2004, October 14). *Protecting your ID – RFID chip in humans get green light*. Retrieved May 13, 2006, from <http://www.silicon.com/research/specialreports/protectingid/0,3800002220,39124983,00.htm>
- Hannibal (2004, October 13). *FDA approves implanted RFID chip for humans*. Message posted to <http://arstechnica.com/news.ars/post/20041013-4305.html>
- Hesseldahl, A. (2004, July 29). *A hacker’s guide to RFID*. Retrieved May 21, 2006, from http://www.forbes.com/business/commerce/2004/07/29/cx_ah_0729rfid.html
- Ho, L., et al (2005, August 22-26). *A prototype on RFID and sensor networks for elder healthcare: Progress report*. *Communications of the ACM*, 70-75. Retrieved May 19, 2006, from the ACM Digital Library database.
- Homeland security RFI heightens public concerns over RFID*. (2006, February 21). Retrieved May 13, 2006, from <http://www.spychips.com/press-releases/dhs-rfid.html>
- Horn, T. (2005). *From microchips to the mark of the beast*. Retrieved May 19, 2006, from <http://www.conspiracyplanet.com/channel.cfm?channelid=74&contentid=3346>

- Hostetter, D. (2005, December 16). *When small technology is a big deal: Legal issues arising from business use of RFID*. Retrieved May 19, 2006, from <http://www.lctjournal.washington.edu/Vol2/a010Hostetter.html>
- Juels, A., et al (2003, October 27-31). The blocker tag: Selective blocking of RFID tags for consumer privacy. *Communications of the ACM*, 103-111. Retrieved May 19, 2006, from the ACM Digital Library database.
- Kanellos, M. (2004, September 7). *Perspective: RFID tags: The people say no*. Retrieved May 13, 2006, from <http://news.com.com/RFID+tags:+The+people+say+no>
- Kanellos, M. (2005, May 17). *L.A. county jail tags inmates with RFID*. Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- Levary, R., et al (2005, February 14). RFID, electronic eavesdropping and the law. *RFID Journal*. Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/articleview/1401/1/133/>
- Levinson, M. (2003, December 1). *Customers to retailers: Take us seriously*. Retrieved May 13, 2006, from http://www.cio.com/archive/120103/retail_sidebar_2.html
- Levinson, M. (2003, December 1). *The RFID imperative*. Retrieved May 13, 2006, from <http://www.cio.com/archive/120103/retail.html>
- Lundquist, E. (2006, March 22). *The real RFID security issue*. Retrieved May 19, 2006, from <http://www.eweek.com/article2/0,1759,1941421,00.asp>
- Lundquist, E. (2006, March 23). *'Mr. RFID' discusses RFID security*. Retrieved May 19, 2006, from <http://www.eweek.com/article2/0,1759,1941977,00.asp>
- Martins, C. (n.d.). Standards progress – It's all relative. *RFID Journal*. Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/articleview/1674/1/128/>
- McCullagh, D. (2003, January 13). *Perspective: RFID tags: Big brother in small packages*. Retrieved May 13, 2006, from <http://news.com.com/2010-1069-980325.html>
- Miller, L. (2004, November 26). *U.S. opposed passport privacy protections*. Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- Miller, L. (2005, January 25). *Technology could speed border crossings*. Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- Moore, B. (2005, June 30). *Analysis: Counterfeit tags*. Retrieved May 21, 2006, from <http://aimglobal.org/members/news/templates/rfidinsights.asp?articleid=393&zoneid=24>

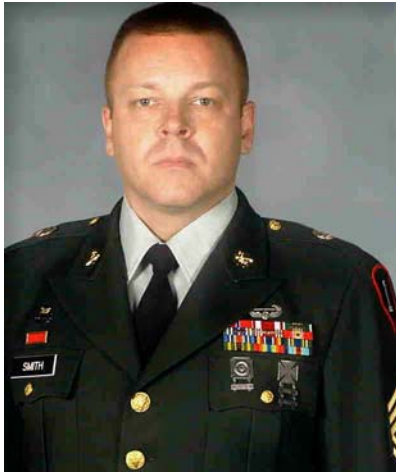
- Moore, B. (2005, October 27). *Spychips: Fact or fiction?* Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/aimpress.asp?articleid=478&zoneid=1>
- Moore, B. (2006, January 5). *Editorial: 2006 -- the year of RFID legislation?* Retrieved May 21, 2006, from <http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=586&zoneid=43>
- Moore, B. (2006, February 2). *Which is better: RFID legislation or RFID guidelines?* Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=667&zoneid=43>
- Moore, B. (2006, February 9). *RFID security: Getting serious.* Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=721&zoneid=43>
- Moore, B. (2006, April 27). *RFID and homeland permeability.* Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=1142&zoneid=43>
- Mullen, D. (2006, May 11). *RFID: For the common good.* Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=1204>
- Murray, C. (2002, January 4). *Injectable chips for people – the “human bar code”.* [<http://eetimes.com/story/OEG20020104S0044>]. Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- Naraine, R. (2006, March 15). *Dutch researchers created RFID malware.* Retrieved May 19, 2006, from <http://www.eweek.com/article2/0,1895,1938391,00.asp>
- Newitz, A. (2006, May 14). *The RFID hacking underground – They can steal your smartcard, lift your passport, jack your car, even clone the chip in your arm. And you won't feel a thing. 5 tales from the RFID-hacking underground.* Retrieved May 19, 2006, from http://www.wired.com/wired/archive/14.05/rfid_pr.html
- New-look passports.* (2005, February 17). Retrieved May 13, 2006, from http://www.economist.com/science/displayStory.cfm?story_id=3666171
- O'Connor, M. (2006, January 2). *The consequences of convenience. RFID Journal.* Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/articleprint/2067/-1/1>
- Pang, A. (2005, July 14). *RFID and religion.* Message posted to http://future.iftf.org/2005/07/rfid_and_religi.html

- Perton, M. (2006, March 13). US issues first RFID passports. Message posted to <http://www.engadget.com/2006/03/13/us-issues-first-rfid-passports/>
- Pescovitz, D. (2005, July 14). RFIDs of the beast, starring Katherine Albrecht. Message posted to http://www.boingboing.net/2005/07/14/rfids_of_the_beast_s.html
- Pescovitz, D. (2006, March 16). Howto make an RFID virus. Message posted to http://www.boingboing.net/2006/03/16/howto_make_an_rfid_v.html
- Privacy Rights Clearinghouse (2003, November 20). *RFID position statement of consumer privacy and civil liberties organizations*. Retrieved May 19, 2006, from <http://www.privacyrights.org/ar/RFIDposition.htm>
- Quirk, R. (2005, April 11). Don't get behind the regulatory eight ball. *RFID Journal*. Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/articleview/1484/1/133/>
- Radio frequency identification (RFID) chips – a key part of the global surveillance society – a technological advancement over Nazi tattooing of prisoners*. (n.d.). Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- Ramasastry, A. (2005, August 12). *Why the 'real ID' act is a real mess*. Retrieved April 17, 2006, from <http://www.cnn.com/2005/LAW/08/12/ramasastry.ids/index.html>
- RFID and privacy laws*. (2005, March 22). Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/rfidinsights.asp?articleid=311&zoid=24>
- RFID – From Wikipedia, the free encyclopedia*. (n.d.). Retrieved May 13, 2006, from <http://en.wikipedia.org/wiki/RFID>
- RFID hacking threat overstated*. (2005, February 15). Retrieved May 13, 2006, from <http://www.aimglobal.org/members/news/templates/aiminsights.asp?articleid=292&zoid=26>
- RFID implants: Fine for thee, but not for me*. (2005, December 7). Retrieved May 13, 2006, from <http://www.spsychips.com/press-releases/verichip-thompson-no-implant.html>
- RFID: No human tracking*. (2006, May 1). Retrieved May 13, 2006, from <http://www.redherring.com/Article.aspx?a=16703&hed=RFID%3A+No+Human+Tracking>

- Roberti, M. (2002, August 12). The privacy nightmare – Only an aggressive PR campaign and an enforceable code of ethics will get people to accept self-regulate of RFID tracking of consumer products. *RFID Journal*. Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/view/144/1/1/>
- Roberti, M. (2004, March 1). The law of the land – Legislation introduced in Utah and California will force companies in the United States to address the privacy issue. *RFID Journal*. Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/articleview/811/>
- Roberti, M. (2004, July 5). Faith in the system, part II – The capitalist system that some privacy advocates think will exploit consumers will, in fact, protect them. *RFID Journal*. Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/articleview/1011/1/2/>
- Schneier, B. (2006, March 16). Schneier on Security – RFID chips and viruses. Message posted to http://www.schneier.com/blog/archives/2006/03/rfid_chips_and_1.html
- Singel, R. (2004, October 21). *American passports to get chipped* [<http://www.wired.com/news/privacy/0,1848,65412,00.html>]. Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- Sotto, L. (2005, May 30). An RFID code of conduct. *RFID Journal*. Retrieved May 19, 2006, from <http://www.rfidjournal.com/article/articleview/1624/1/133/>
- Stajano, F. (2005, September). RFID is x-ray vision. *Communications of the ACM*, 48(9), 31-33. Retrieved May 19, 2006, from the ACM Digital Library database.
- Stapleton-Gray, R. (2005, August 24). *Guest editorial: Privacy invasion as ROI*. Retrieved May 21, 2006, from <http://www.aimglobal.org/members/news/templates/>
- Sterling, B. (2006, March 20). Meanwhile, back in Arphidland [Msg id=1440029]. Message posted to http://wiredblogs.tripod.com/sterling/index.blog?entry_id=1440029
- Sullivan, L. (2006, March 15). Virus allegations rock RFID world. Message posted to http://techsearch.cmp.com/blog/archives/2006/03/melanie_rieback.html?loc=software
- Talbot, D. (2006, May/June). *As part of an information system, even the lowly RFID tag is vulnerable*. Retrieved May 13, 2006, from http://www.technologyreview.com/read_article.aspx?id=16797&ch=infotech
- The pros and cons of RFID. (2005, May). *Strategic Direction*, 21(5), 24-26. Retrieved May 19, 2006, from ABI/Inform Global (ProQuest) database.

- Verichip RFID implant hacked!* (2006, January 27). Retrieved May 13, 2006, from <http://www.spsychips.com/press-releases/verichip-hacked.html>
- Vrije Universiteit Amsterdam. (2006). *Is your cat infected with a computer virus?* Retrieved May 19, 2006, from the Vrije Universiteit Amsterdam Faculty of Sciences Web site: <http://www.rfidvirus.org/>
- Wagstaff, J. (2006, March 16). How to infect an airport. Message posted to http://www.loosewireblog.com/2006/03/how_to_infect_a.html
- Wald, M. (2004). *Electronic passports raise privacy fears*. Retrieved May 13, 2006, from <http://www.oilempire.us/rfid.html>
- Want, R. (2004, October). The magic of RFID. *Queue*, 41-48. Retrieved May 19, 2006, from the ACM Digital Library database.
- Weiss, A. (2003, September). Me and my shadow. *Communications of the ACM*, 25-30. Retrieved May 19, 2006, from the ACM Digital Library database.

AUTHOR'S NOTE



David B. Smith is a Sergeant First Class (E-7) in the U.S. Army. He currently works at the Office of the Judge Advocate, U.S. Army Europe & 7th Army, in Heidelberg, Germany. He will be retiring November 1, 2006, after a 21 year career as an Army Paralegal. During his career, he has been stationed in various locations throughout Europe, the United States and Asia. His training includes the Legal Specialist course, Primary Leadership Development course, Basic and Advanced Noncommissioned Officer courses, Military Paralegal Program, Total Army Instructor Training course, Training Management course, Supervisor Development course, Knowledge Management course, Information Assurance Security Officer course, and Information Assurance/Computer Network Defense I & II courses. He holds certifications as an Army Instructor and Information Systems Analyst. Questions and comments about this research paper should be sent via e-mail to david.b.smith@us.army.mil (please do not forward jokes, chain letters or other items considered to be spam or bulk e-mail to this address).